Combinatorics

Instructor: Jie Ma, Scribed by Jun Gao, Jialin He and Tianchi Yang

2020 Fall, USTC

Contents

1 Enumeration

First we give some standard notation that will be used throughout this course. Let n be a positive integer. We will use $[n]$ to denote the set $\{1, 2, ..., n\}$. Given a set X, $|X|$ denotes the number of elements contained in X. Sometimes we also use "#" to express the word "number". The *factorial* of n is the product

$$n! = n \cdot (n-1) \cdots 2 \cdot 1,$$

which can be extended to all non-negative integers by letting $0! = 1$.

1.1 Binomial Coefficients

Let X be a set of size n. Define $2^X = \{A : A \subseteq X\}$ to be the family of all subsets of X. So $|2^X| = 2^{|X|} = 2^n$. Let $\binom{X}{k} = \{A : A \subseteq X, |A| = k\}$.

Fact 1.1. *For integers $n > 0$ and $0 \le k \le n$, we have $|\binom{X}{k}| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.*

Proof. If $k = 0$, then it is clear that $|\binom{X}{0}| = |\{\emptyset\}| = 1 = \binom{n}{0}$. Now we consider $k > 0$. Let

$$(n)_k := n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

First we will show that number of ordered k-tuples $(x_1, x_2, ..., x_k)$ with distinct $x_i \in X$ is $(n)_k$. There are n choices for the first element x_1. When $x_1, ..x_i$ is chosen, there are exactly $n - i$ choices for the element x_{i+1}. So the number of ordered k-tuples $(x_1, x_2, ..., x_k)$ with distinct $x_i \in X$ is $(n)_k$. Since any subset $A \in \binom{X}{k}$ correspond to $k!$ ordered k-tuples, it follows that $|\binom{X}{k}| = \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}$. This finishes the proof. ∎

Next we discuss more properties of binomial coefficients. For a positive integer n strictly less than k, we let $\binom{n}{k} = 0$.

Fact 1.2. (1). $\binom{n}{k} = \binom{n}{n-k}$ *for* $0 \le k \le n$.
(2). $2^n = \sum_{0 \le k \le n} \binom{n}{k}$.
(3). $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Proof. (1) is trivial. Since $2^{[n]} = \cup_{0 \le k \le n} \binom{[n]}{k}$, we see $2^n = \sum_{0 \le k \le n} \binom{n}{k}$, proving (2). Finally, we consider (3). Note that the first term on the right hand side $\binom{n-1}{k-1}$ is the number of k-sets containing a fixed element, while the second term $\binom{n-1}{k}$ is the number of k-sets avoiding this element. So their summation gives the total number of k-sets in $[n]$, which is $\binom{n}{k}$. This finishes the proof. ∎

Pascal's triangle is a triangular array constructed by summing adjacent elements in preceding rows. By Fact 1.2 (3), in the following graph we have that the k-th element in the n row is $\binom{n}{k-1}$.

1 ································ 1 1
2 ······························ 1 2 1
3 ···························· 1 3 3 1
4 ·························· 1 4 6 4 1
5 ························ 1 5 10 10 5 1
6 ······················ 1 6 15 20 15 6 1
7 ···················· 1 7 21 35 35 21 7 1
8 ················ 1 8 28 56 70 56 28 8 1
9 ·············· 1 9 36 84 126 126 84 36 9 1
10 ·········· 1 10 45 120 210 252 210 120 45 10 1

Fact 1.3. *The number of integer solutions $(x_1, ..., x_n)$ to the equation $x_1 + \cdots x_n = k$ with each $x_i \in \{0, 1\}$ is $\binom{n}{k}$.*

Fact 1.4. *The number of integer solution $(x_1, ...x_n)$ with each $x_i \ge 0$, to the equation $x_1 + \cdots x_n = k$ is $\binom{n+k-1}{n-1}$.*

Proof. Suppose we have k sweets (of the same sort), which we want to distribute to n children. In how many ways can we do this? Let x_i denote the number of sweets we give to the i-th child, this question is equivalent to that state above.

We lay out the sweets in a single row of length r and let the first child pick them up from left to right (can be 0). After a while we stop him/her and let the second child pick up sweets, etc. The distribution is determined by the specifying the place of where to start a new child. Equal to select $n - 1$ elements from $n + r - 1$ elements to be the child, others be the sweets (the first child always starts at the beginning). So the answer is $\binom{n+k-1}{n-1}$. ∎

Exercise 1.5. *Prove that*

$$\sum_{k=0}^{m} \binom{m}{k} \binom{n+k}{m} = \sum_{k=0}^{m} \binom{n}{k} \binom{m}{k} 2^k.$$

1.2 Counting Mappings

Define X^Y to be the set of all functions $f : Y \to X$.

Fact 1.6. $|X^Y| = |X|^{|Y|}$.

Proof. Let $|Y| = r$. We can view X^Y as the set of all strings $x_1 x_2 ... x_r$ with elements $x_i \in X$, indexed by the r element of Y. So $|X^Y| = |X|^{|Y|}$. ∎

Fact 1.7. *The number of injective functions $f : [r] \to [n]$ is $(n)_r$.*

Proof. We can view the injective function f as a ordered k-tuples $(x_1, x_2, ..., x_r)$ with distinct $x_i \in X$, so the number of injective functions $f : [r] \to [n]$ is $(n)_r$. ∎

Definition 1.8 (The Stirling number of the second kind). *Let S(r,n) be the number of partition of $[r]$ into n unordered non-empty parts.*

Exercise 1.9. *Prove that*

$$S(r, 2) = \frac{2^r - 2}{2} = \frac{1}{2}\sum_{i=1}^{r-1}\binom{r}{i}.$$

Fact 1.10. *The number of surjective functions $f : [r] \to [n]$ is $n!S(r, n)$.*

Proof. Since f is a surjective function if and only if for any $i \in [n], f^{-1}(i) \neq \emptyset$ if and only if $\cup_{i\in[n]} f^{-1}(i) = [r]$, and $S(r, n)$ is the number of partition of $[r]$ into n unordered non-empty parts, we have the number of surjective functions $f : [r] \to [n]$ is $n!S(r, n)$. ∎

We say that any injective $f : X \to X$ is a **permutation** of X (also a bijection). We may view a permutation in two ways: (1) it is a bijective from X to X. (2) a reordering of X.

Cycle notation describes the effect of repeatedly applying the permutation on the elements of the set. It expresses the permutation as a product of cycles; since distinct cycles are disjoint, this is referred to as "decomposition into disjoint cycles".

Definition 1.11. *The Stirling number of the first kind $s(r, n)$ is $(-1)^{(r-n)}$ times the number of permutations of $[r]$ with exactly n cycles.*

The following fact is a direct consequence of Fact 1.7.

Fact 1.12. *The number of permutation of $[n]$ is $n!$.*

Exercise 1.13. *(1) Let $S(r, n) = \left\{ {r \atop n} \right\}$. Then $\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$. (give a Combinatorial proof.)*

(2) Let $s(n, k) = (-1)^{n-k} \left[{n \atop k} \right]$. Then $\left[{n \atop k} \right] = \left[{n-1 \atop k-1} \right] + (n-1) \left[{n-1 \atop k} \right]$

1.3 The Binomial Theorem

Define $[x^k]f$ to be the coefficient of the term x^k in the polynomial $f(x)$.

Fact 1.14. *For $j = 1, 2, ..., n$, let $f_j(x) = \sum_{k\in I_j} x^k$ where I_j is a set of non-negative integers, and let $f(x) = \prod_{j=1}^{n} f_j(x)$. Then, $[x^k]f$ equals the number of solutions $(i_1, i_2, ..., i_n)$ to $i_1+i_2+...+i_n = k$, where $i_j \in I_j$.*

Fact 1.15. *Let $f_1, ..., f_n$ be polynomials and $f = f_1 f_2 ... f_n$. Then,*

$$[x^k]f = \sum_{i_1+\cdots+i_n=k, i_j\geq 0} \left(\prod_{j=1}^{n} [x^{i_j}] f_j \right).$$

Theorem 1.16 (The Binomial Theorem)**.** *For any real x and any positive integer n, we have*

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i.$$

Proof 1. Let $f = (1+x)^n$. By Fact 1.14 we have $[x^k]f$ equals the number of solutions $(i_1, i_2, ..., i_n)$ to $i_1 + i_2 + ... + i_n = k$ where $i_j \in \{0, 1\}$, so $[x^k]f = \binom{n}{k}$. ∎

Proof 2. By induction on n. When $n = 1$, it is trivial. If the result holds for $n-1$, then $(1+x)^n = (1+x)(1+x)^{n-1} = (1+x)\sum_{i=0}^{n-1}\binom{n-1}{i}x^i = \sum_{i=1}^{n-1}(\binom{n-1}{i} + \binom{n-1}{i-1})x^i + 1 + x^n$. Since $\binom{n-1}{i} + \binom{n-1}{i-1} = \binom{n}{i}$ and $\binom{n}{0} = \binom{n}{n} = 1$, we have $(1+x)^n = \sum_{i=0}^{n}\binom{n}{i}x^i$. ∎

Fact 1.17. $\binom{2n}{n} = \sum_{i=0}^{n}\binom{n}{i}^2 = \sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}$.

Proof 1. Since $(1+x)^{2n} = (1+x)^n(1+x)^n$, by Fact 1.15, we have $\binom{2n}{n} = [x^n](1+x)^{2n} = \sum_{i=0}^{n}([x^i](1+x)^n)([x^{n-i}](1+x)^n) = \sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i} = \sum_{i=0}^{n}\binom{n}{i}^2$. ∎

Proof 2. (It is easy to find a combinatorial proof.) ∎

Exercise 1.18 (Vandermonde's Convolution Formula)**.**

$$\binom{n+m}{k} = \sum_{j=0}^{k}\binom{n}{j}\binom{m}{k-j}.$$

Fact 1.19. (1).

$$\sum_{\textit{all even } k}\binom{n}{k} = \sum_{\textit{all odd } k}\binom{n}{k} = 2^{n-1}.$$

(2).

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

Proof. (1). We see that $(1+x)^n = \sum_{i=0}^{n}\binom{n}{i}$. Taking $x = 1$ and $x = -1$, we have

$$\sum_{\text{all even } k}\binom{n}{k} = \sum_{\text{all odd } k}\binom{n}{k} = 2^{n-1}.$$

(2). Let $f(x) = (1+x)^n = \sum_{k=0}^{n} x^k$. Then $f'(x) = n(1+x)^{n-1} = \sum_{k=0}^{n} k\binom{n}{k}x^{k-1}$. Let $x = 1$, then we have $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$. ∎

Definition 1.20. *Let $k_j \geq 0$ be integers satisfying that $k_1 + k_2 + \cdots + k_m = n$. We define*

$$\binom{n}{k_1, k_2, ..., k_m} := \frac{n!}{k_1!k_2!...k_m!}.$$

The following theorem is a generalization of the binomial theorem.

Theorem 1.21 (Multinomial Theorem). *For any reals $x_1, ..., x_m$ and any positive integer $n \geq 1$, we have*

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1+k_2+\cdots+k_m=n,\ k_j \geq 0} \binom{n}{k_1, k_2, ..., k_m} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}.$$

Proof. Omit. ∎

Exercise 1.22. *Suppose $\sum_{i=1}^m k_i = n$ with $k_i \geq 1$ for all $i \in m$. Then*

$$\binom{n}{k_1, k_2, ..., k_m} = \binom{n-1}{k_1 - 1, k_2, ..., k_m} + \cdots + \binom{n-1}{k_1, k_2, ..., k_m - 1}.$$

1.4 Estimating Binomial Coefficients

Theorem 1.23. *For any integer $n \geq 1$, we have*

$$e \left(\frac{n}{e}\right)^n \leq n! \leq en \left(\frac{n}{e}\right)^n, \tag{1.1}$$

where $e = \lim\limits_{n\to\infty} (1 + \frac{1}{n})^n$ is the Euler number.

Proof. We have

$$\ln(n!) = \sum_{i=1}^n \ln i \leq \int_1^{n+1} \ln x \, dx = (x \ln x - x)\Big|_{x=1}^{x=n+1} = (n+1)\ln(n+1) - n.$$

Then it follows that

$$n! \leq \frac{(n+1)^{n+1}}{e^n}.$$

Reset $n = n - 1$, we have

$$(n-1)! \leq \frac{n^n}{e^{n-1}} \iff n! \leq ne \left(\frac{n}{e}\right)^n.$$

Similarly we have

$$\ln(n!) \geq \int_1^n \ln x \, dx = (x \ln x - x)\Big|_1^n = n \ln n - (n-1),$$

which implies that

$$n! \geq \frac{n^n}{e^{n-1}} = e \left(\frac{n}{e}\right)^n,$$

as desired. ∎

Modifying the above proof, we can obtain the following improvement.

Exercise 1.24. *Prove that*

$$n! \le e\sqrt{n}\left(\frac{n}{e}\right)^n.$$

Definition 1.25. *Define $f \sim g$ for functions f and g, if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$.*

The following formula is well-known.

Theorem 1.26 (Stirling's formula.). $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$.

It is easy to show the following two facts.

Fact 1.27. *Let n be a fix integer. We can view $\binom{n}{k}$ as a function with $k \in \{0, 1, 2, ..., n\}$. It is increasing when $k \le \lfloor \frac{n}{2} \rfloor$, and decreasing when $k > \lfloor \frac{n}{2} \rfloor$. Therefore, $\binom{n}{k}$ achievers its maximum at $k = \lfloor \frac{n}{2} \rfloor$ or $\lceil \frac{n}{2} \rceil$.*

Fact 1.28. $\frac{2^n}{n} \le \binom{n}{\lfloor \frac{n}{2} \rfloor} \le 2^n$

Exercise 1.29. *For any even integer $n > 0$, we have*

$$\frac{2^n}{\sqrt{2n}} \le \binom{n}{n/2} \le \frac{2^n}{\sqrt{n}}.$$

If we are allowed to use Stirling's formula, then we can get

$$\binom{n}{\frac{n}{2}} \sim \sqrt{\frac{2}{\pi}} \frac{2^n}{\sqrt{n}}.$$

Fact 1.30. $\binom{n}{k} = \frac{(n)_k}{k!} \le \frac{n^k}{k!}$.

Exercise 1.31. $1 + x \le e^x$ *holds for any real x.*

Theorem 1.32. *For any integers $1 \le k \le n$, we have $(\frac{n}{k})^k \le \binom{n}{k} \le (\frac{en}{k})^k$.*

Proof. Since $\frac{n-i}{k-i} \ge \frac{n}{k}$ for each $0 \le i \le k-1$, we have

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k \cdot (k-1) \cdots 1} = \left(\frac{n}{k}\right) \cdot \left(\frac{n-1}{k-1}\right) \cdots \left(\frac{n-k+1}{k}\right) \ge \left(\frac{n}{k}\right)^k.$$

For the upper bound, since $k! \ge e(\frac{k}{e})^k > (\frac{k}{e})^k$, by Fact 1.30 we have

$$\binom{n}{k} \le \frac{n^k}{k!} \le \left(\frac{en}{k}\right)^k,$$

as desired. ∎

We can also prove the following strengthening.

Theorem 1.33. *For any integers $1 \le k \le n$,*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \le \left(\frac{en}{k}\right)^k.$$

Proof. By the binomial theorem, we have

$$\binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{k}x^k \leq (1+x)^n$$

for any $0 < x \leq 1$. Then for any $0 < x \leq 1$, it gives that

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{\binom{n}{0}}{x^k} + \frac{\binom{n}{1}}{x^{k-1}} + \cdots + \frac{\binom{n}{k}}{1} \leq \frac{(1+x)^n}{x^k}.$$

Taking $x = \frac{k}{n} \in (0, 1]$, we have

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k} \leq \frac{e^{xn}}{x^k} = \left(\frac{en}{k}\right)^k,$$

as desired. ∎

1.5 Inclusion and Exclusion

This lecture is devoted to Inclusion-Exclusion formula and its applications.

Let Ω be a ground set and let $A_1, A_2, ..., A_n$ be subsets of Ω. Write $A_i^c = \Omega \backslash A_i$. Throughout this lecture, we use the following notation.

Definition 1.34. *Let $A_\emptyset = \Omega$. For any nonempty subset $I \subseteq [n]$, let*

$$A_I = \bigcap_{i \in I} A_i.$$

For any integer $k \geq 0$, let

$$S_k = \sum_{I \in \binom{[n]}{k}} |A_I|.$$

Now we introduce Inclusion-Exclusion formula (in three equivalent forms) and give two proofs as following.

Theorem 1.35 (Inclusion-Exclusion Formula)**.** *We have*

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} S_k,$$

which is equivalent to to

$$\left| \Omega \backslash \bigcup_{i=1}^{n} A_i \right| = |A_1^c \cap A_2^c \cap ... \cap A_n^c| = \sum_{k=0}^{n} (-1)^k S_k,$$

i.e.,

$$\left| \Omega \backslash \bigcup_{i=1}^{n} A_i \right| = |A_1^c \cap A_2^c \cap ... \cap A_n^c| = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I|.$$

Proof (1). For any subset $X \subseteq \Omega$, we define its characterization function $\mathbb{1}_X : \Omega \to \{0,1\}$ by assigning

$$\mathbb{1}_X(x) = \begin{cases} 1, & x \in X \\ 0, & x \notin X. \end{cases}$$

Then $\sum_{x\in\Omega} \mathbb{1}_X(x) = |X|$. Let $A = A_1 \cup A_2 \cup ... \cup A_n$. Our key observation is that

$$(\mathbb{1}_A - \mathbb{1}_{A_1})(\mathbb{1}_A - \mathbb{1}_{A_2}) \cdots (\mathbb{1}_A - \mathbb{1}_{A_n})(x) \equiv 0$$

holds for any $x \in \Omega$. Next we expand this product into a summation of 2^n terms as following:

$$\sum_{I\subseteq[n]} (-1)^{|I|}(\prod_{i\in I} \mathbb{1}_{A_i}) \equiv 0 \iff \mathbb{1}_A(x) + \sum_{I\subseteq[n],\ I\neq\emptyset} (-1)^{|I|}\mathbb{1}_{A_I}(x) \equiv 0$$

holds for any $x \in \Omega$. Summing over all $x \in \Omega$, this gives that

$$|A| + \sum_{I\subseteq[n],\ I\neq\emptyset} (-1)^{|I|}|A_I| = 0,$$

which implies that

$$|A_1 \cup A_2 \cup ... \cup A_n| = |A| = \sum_{\substack{I\subseteq[n]\\ I\neq\emptyset}} (-1)^{|I|+1}|A_I| = \sum_{k=1}^{n}(-1)^{k+1}S_k,$$

finishing the proof. ∎

Proof (2). It suffices to prove that

$$\mathbb{1}_{A_1\cup A_2\cup...\cup A_n}(x) = \sum_{k=1}^{n}(-1)^{k+1} \sum_{I\in\binom{[n]}{k}} \mathbb{1}_{A_I}(x)$$

holds for all $x \in \Omega$. Denote by LHS (resp. RHS) the left (resp. right) side of the above equation.

Assume that x is contained in exactly ℓ subsets, say $A_1, A_2, \cdots, A_\ell$. If $\ell = 0$, then clearly $LHS = 0 = RHS$, so we are done. So we may assume that $\ell \geq 1$. In this case, we have $LHS = 1$ and

$$RHS = \ell - \binom{\ell}{2} + \binom{\ell}{3} + \cdots + (-1)^{\ell+1}\binom{\ell}{\ell} = 1.$$

Note that the above equation holds since $\sum_{i=0}^{\ell}(-1)^i\binom{\ell}{i} = (1-1)^\ell = 0$. This finishes the proof. ∎

Next, we will demonstrate the power of Inclusion-Exclusion formula by using it to solve several problems.

Definition 1.36. *Let $\varphi(n)$ be the number of integers $m \in [n]$ which are relatively prime*[1] *to n.*

[1]Here, "m is relatively prime to n" means that the greatest common divisor of m and n is 1.

Theorem 1.37. *If we express $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, where $p_1 \cdots p_t$ are distinct primes, then*

$$\varphi(n) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i}).$$

Proof. Let $A_i = \{m \in [n] : p_i | m\}$ for $i \in \{1, 2, \cdots, t\}$. It implies

$$\varphi(n) = \left|\{m \in [n] : m \notin A_i \text{ for all } i \in [t]\}\right| = \left|[n] \backslash (A_1 \cup A_2 \cup \cdots \cup A_t)\right|.$$

By Inclusion-Exclusion formula,

$$\varphi(n) = \sum_{I \subseteq [t]} (-1)^{|I|} |A_I|,$$

where $A_I = \cap_{i \in I} A_i = \{m \in [n] : (\prod_{i \in I} p_i) | m\}$ and thus $|A_I| = n / \prod_{i \in I} p_i$. We can derive that

$$\varphi(n) = \sum_{I \subseteq [t]} (-1)^{|I|} \frac{n}{\prod_{i \in I} p_i} = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_t}),$$

as desired. ∎

Definition 1.38. *A permutation $\sigma : [n] \to [n]$ is called a* **derangement** *of $[n]$ if $\sigma(i) \neq i$ for all $i \in [n]$.*

Theorem 1.39. *Let D_n be the family of all derangement of $[n]$. Then*

$$|D_n| = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Proof. Let

$$A_i = \{\text{all permutations } \sigma : [n] \to [n] \text{ such that } \sigma(i) = i\}.$$

Then

$$D_n = A_1^c \cap A_2^c \cap \cdots \cap A_n^c \text{ and } |A_I| = (n - |I|)!.$$

By Inclusion-Exclusion formula, we get

$$|D_n| = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!},$$

as desired. ∎

Remark 1.40. *We have that*

$$|D_n| \to \frac{n!}{e} \text{ as } n \to \infty.$$

It is because $\sum_{k=0}^{+\infty} \frac{(-1)^k}{k!} = e^{-1}$ (by the Taylor series of $e^x = \sum_{k=0}^{+\infty} \frac{x^k}{k!}$).

Next we recall the definition of $S(n, k)$ and aim to give a precise formula for it. We know that

(1.) $S(n,k)$ is equal to the number of partitions of $[n]$ into k non-ordered non-empty set.

(2.) $S(n,k)k!$ is equal to the number of surjective functions $f:[n]\to[k]$.

Theorem 1.41. *We have*

$$S(n,k)=\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n.$$

Proof. For $i\in[k]$, let

$$A_i=\{\text{all functions } f:[n]\to[k]\backslash\{i\}\}.$$

Then

$$A_1^c\cap A_2^c\cap\cdots\cap A_k^c=\{\text{all surjective } f:[n]\to[k]\}.$$

So

$$S(n,k)k!=\text{ the number of surjective } f:[n]\to[k]=\sum_{i=0}^{k}(-1)^iS_i,$$

where

$$S_i=\sum_{I\in\binom{[k]}{i}}|A_I|=\binom{k}{i}(k-i)^n.$$

Finally, we get

$$S(n,k)=\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n.$$

∎

1.6 Generating Functions

Definition 1.42. *The (ordinary)* **generating function** *for an infinity sequence* $\{a_0,a_1,\cdots\}$ *is a power series*

$$f(x)=\sum_{n\geq 0}a_nx^n.$$

We have two ways to view this power series.

(i). When the power series $\sum_{n\geq 0}a_nx^n$ converges (i.e. there exists a radius $R>0$ of convergence), we view GF as a function of x and we can apply operations of calculus on it (including differentiation and integration). For example, we know that

$$a_n=\frac{f^{(n)}(0)}{n!}.$$

Recall the following sufficient condition on the radius of convergence that if $|a_n|\leq K^n$ for some $K>0$, then $\sum_{n\geq 0}a_nx^n$ converges in the interval $(-\frac{1}{K},\frac{1}{K})$.

(ii). When we are not sure of the convergence, we view the generating function as a formal object with additions and multiplications. Let $a(x) = \sum_{n\geq 0} a_n x^n$ and $b(x) = \sum_{n\geq 0} b_n x^n$.

Addition.

$$a(x) + b(x) = \sum_{n\geq 0}(a_n + b_n)x^n.$$

Multiplication. Let $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. Then

$$a(x)b(x) = \sum_{n\geq 0} c_n x^n.$$

Example 1.43. *We see $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ holds for all $-1 < x < 1$. By the point view of (i), its first derivative gives*

$$\frac{1}{(1-x)^2} = \sum_{n=1}^{\infty} nx^{n-1} = \sum_{n=0}^{\infty}(n+1)x^n.$$

Problem 1.44. *Let $a_0 = 1$ and $a_n = 2a_{n-1}$ for $n \geq 1$. Find a_n.*

Solution. Consider the generating function,

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = 1 + \sum_{n=1}^{\infty} a_n x^n = 1 + 2x\sum_{n=1}^{\infty} a_{n-1}x^{n-1} = 1 + 2xf(x).$$

So $f(x) = \frac{1}{1-2x}$, which implies that $f(x) = \sum_{n=0}^{+\infty} 2^n x^n$ and $a_n = 2^n$. ∎

From this problem, we see one of the basic ideas for using generating function: in order to find the general expression of a_n, we work on its generating function $f(x)$; once we find the formula of $f(x)$, then we can expand $f(x)$ into a power series and get a_n by choosing the coefficient of the right term.

Fact 1.45. *For $j \in [n]$, let $f_j(x) := \sum_{i\in I_j} x^i$, where $I_j \subset Z$. Let b_k be the number of solutions to $i_1 + i_2 + ... + i_n = k$ for $i_j \in I_j$. Then*

$$\prod_{j=1}^{n} f_j(x) = \sum_{k=0}^{\infty} b_k x^k.$$

Fact 1.46. *If $f(x) = \prod_{i=1}^{k} f_i(x)$ for polynomials $f_1, ..., f_k$, then*

$$[x^n]f = \sum_{i_1+i_2+\cdots+i_k=n} \prod_{j=1}^{k}\left([x^{i_j}]f_j\right),$$

where $[x^n]f$ is the coefficient of x^n in f.

Problem 1.47. *Let A_n be the set of strings of length n with entries from the set $\{a, b, c\}$ and with no "aa" occuring (in the consecutive positions). Find $|A_n|$ for $n \geq 1$.*

Solution. Let $a_n = |A_n|$. We first observe that $a_1 = 3, a_2 = 8$. For $n \geq 3$, we will find a_n by recursion as following. If the first string is 'a', the second string has two choices, 'b' or 'c'. Then the last $n-2$ strings have a_{n-2} choices. If the first string is 'b' or 'c', the last $n-1$ strings have a_{n-1} choices. They are all different. Totally, for $n \geq 3$, we have

$$a_n = 2a_{n-1} + 2a_{n-2}.$$

Set $a_0 = 1$, then $a_n = 2a_{n-1} + 2a_{n-2}$ holds for $n \geq 2$. The generating function of $\{a_n\}$ is

$$f(x) = \sum_{n\geq 0} a_n x^n = a_0 + a_1 x + \sum_{n\geq 2}(2a_{n-1} + 2a_{n-2})x^n = 1 + 3x + 2x(f(x) - 1) + 2x^2 f(x),$$

which implies that

$$f(x) = \frac{1+x}{1-2x-2x^2}.$$

By Partial Fraction Decomposition, we calculate that

$$f(x) = \frac{1-\sqrt{3}}{2\sqrt{3}} \frac{1}{\sqrt{3}+1+2x} + \frac{1+\sqrt{3}}{2\sqrt{3}} \frac{1}{\sqrt{3}-1-2x},$$

which implies that

$$a_n = \frac{1-\sqrt{3}}{2\sqrt{3}} \frac{1}{\sqrt{3}+1} \left(\frac{-2}{\sqrt{3}+1}\right)^n + \frac{1+\sqrt{3}}{2\sqrt{3}} \frac{1}{\sqrt{3}-1} \left(\frac{2}{\sqrt{3}-1}\right)^n.$$

Note that a_n must be an integer but its expression is of a combination of irrational terms! Observe that $\left|\frac{-2}{\sqrt{3}+1}\right| < 1$, so $\left(\frac{-2}{\sqrt{3}+1}\right)^n \to 0$ as $n \to \infty$. Thus, when n is sufficiently large, this integer a_n is about the value of the second term $\frac{1+\sqrt{3}}{2\sqrt{3}} \frac{1}{\sqrt{3}-1} \left(\frac{2}{\sqrt{3}-1}\right)^n$. Equivalently a_n will be the nearest integer to that. ∎

Definition 1.48. *For any real r and an integer $k \geq 0$, let*

$$\binom{r}{k} = \frac{r(r-1)...(r-k+1)}{k!}.$$

Theorem 1.49 (Newton's Binomial Theorem)**.** *For any real number r and $x \in (-1, 1)$,*

$$(1+x)^r = \sum_{k=0}^{\infty} \binom{r}{k} x^k.$$

Proof. By Taylor series, it is obvious. ∎

Corollary 1.50. *Let $r = -n$ for some integer $n \geq 0$. Then*

$$\binom{-n}{k} = \frac{(-n)(-n-1)\cdots(-n-k+1)}{k!} = (-1)^k \binom{n+k-1}{k}.$$

Therefore

$$(1+x)^{-n} = \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{k} x^k.$$

Problem 1.51. *Let a_n be the number of ways to pay n Yuan using 1-Yuan bills, 2-Yuan bills and 5-Yuan bills. What is the generating function of this sequence $\{a_n\}$?*

Solution. Observe that a_n is the number of integer solutions (i_1, i_2, i_3) to $i_1 + i_2 + i_3 = n$, where $i_1 \in I_1 := \{0, 1, 2, ...\}$, $i_2 \in I_2 := \{0, 2, 4, ...\}$ and $i_3 \in I_3 := \{0, 5, 10, ...\}$. Let $f_j(x) := \sum_{m \in I_j} x^m$ for $j = 1, 2, 3$. By Fact 1.45, we have

$$\sum_{n=0}^{+\infty} a_n x^n = f_1(x) f_2(x) f_3(x) = \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^5}.$$

∎

1.7 Integer Partitions

How many ways are there to write a natural number n as a sum of several natural numbers? The total number of *ordered partitions* of n is $\sum_{1 \le k \le n} \binom{n-1}{k-1} = 2^{n-1}$. Here "ordered partition" means that we will view $1+1+2, 1+2+1$ as two different partitions of 4.

We then consider the *unordered partitions*. For instance, we will view $1+2+3$ and $3+2+1$ of 6 as the same one.

Let p_n be the number of unordered partitions of n. So $p_1 = 1$, $p_2 = 2$, $p_3 = 3$ and $p_4 = 5$. We have the following theorem.

Theorem 1.52. *The generating function $P(x)$ of $\{p_n\}_{n \ge 0}$ is an infinite product of polynomials*

$$P(x) = \prod_{k=1}^{+\infty} \frac{1}{1-x^k}.$$

Proof. Let n_j be the number of the j's in such a partition of n. Then it holds that

$$\sum_{j \ge 1} j \cdot n_j = n.$$

If we use i_j to express the contribution of the addends equal to j in a partition of n (i.e., $i_j = j \cdot n_j$), then

$$\sum_{j \ge 1} i_j = n, \quad \text{where } \ i_j \in \{0, j, 2j, 3j, ...\}.$$

Note that in the above summation, j can run from 1 to infinity, or run from 1 to n. So by the fact we discussed earlier, p_n is the coefficient of x^n in the product

$$P(x) = (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots) \cdots (1 + x^n + x^{2n} + \cdots) \cdots = \prod_{k=1}^{+\infty} \frac{1}{1-x^k}.$$

This finishes the proof of this theorem. ∎

1.8 The Catalan Number

First let us recall the definition of $\binom{r}{k}$ for real numbers r and positive integers k, and the Newton's binomial Theorem. We obtained that

$$\binom{\frac{1}{2}}{k} = \frac{(-1)^{k-1}2}{4^k} \cdot \frac{(2k-2)!}{k!(k-1)!}.$$

Let n-gon be a polygon with n corners, labeled as corner 1, corner 2,..., corner n.

Definition 1.53. *A triangulation of the n-gon is a way to add lines between corners to make triangles such that these lines do not cross inside of the polygon.*

Then we have the following theorem.

Theorem 1.54. *The total number of triangulations of the $(k+2)$-gon is $\frac{1}{k+1}\binom{2k}{k}$, which is also called* **the k^{th} Catalan number**.

Proof. Let b_{n-1} be the number of triangulations of the n-gon, for $n \geq 3$. It is not hard to see that $b_2 = 1, b_3 = 2, b_4 = 5$. We want to find a general formula of b_n.

Consider the triangle T in a triangulation of n-gon which contains corners 1 and 2. The triangle T should contain a third corner, say i, where $3 \leq i \leq n$. We have the following two cases.

Case 1. If $i = 3$ or n, the triangle T divides the n-gon into the triangle T itself plus an $(n-1)$-gon, which results in b_{n-2} triangulations of n-gon.

Case 2. For $4 \leq i \leq n-1$, the triangle T divides the n-gon into three regions: an $(n-i+2)$-gon, triangle T and an $(i-1)$-gon, therefore it results in $b_{i-2} \times b_{n-i+1}$ many triangulations of n-gon.

Therefore, combining Cases 1 and 2, we get that

$$b_{n-1} = b_{n-2} + \sum_{i=4}^{n-1} b_{i-2}b_{n-i+1} + b_{n-2} = b_{n-2} + \sum_{j=2}^{n-3} b_j b_{n-j-1} + b_{n-2}.$$

By letting $b_0 = 0$ and $b_1 = 1$, we get

$$b_{n-1} = \sum_{j=0}^{n-1} b_j b_{n-1-j} \quad \text{for} \quad n \geq 3 \qquad \text{or} \qquad b_k = \sum_{j=0}^{k} b_j b_{k-j} \quad \text{for} \quad k \geq 2.$$

Let $f(x) = \sum_{k\geq 0} b_k x^k$. Note that $f^2(x) = \sum_{k\geq 0}\left(\sum_{j=0}^{k} b_j b_{k-j}\right)x^k$. Therefore

$$f(x) = x + \sum_{k\geq 2} b_k x^k = x + \sum_{k\geq 2}\left(\sum_{j=0}^{k} b_j b_{k-j}\right)x^k = x + \sum_{k\geq 0}\left(\sum_{j=0}^{k} b_j b_{k-j}\right)x^k = x + f^2(x).$$

Solving $f^2(x) - f(x) + x = 0$, we get that $f(x) = \frac{1+\sqrt{1-4x}}{2}$ or $\frac{1-\sqrt{1-4x}}{2}$. But notice that $f(0) = 0$, so it has to be the case that

$$f(x) = \frac{1-\sqrt{1-4x}}{2}.$$

Next, we apply the Newton's binomial theorem to get that

$$f(x) = \frac{1}{2} - \frac{1}{2}\sum_{k\geq 0}\binom{\frac{1}{2}}{k}(-4x)^k = \sum_{k\geq 1}\frac{(-1)^{k+1}4^k}{2}\binom{\frac{1}{2}}{k}x^k.$$

After plugging the obtained expression of $\binom{\frac{1}{2}}{k} = \frac{(-1)^{k-1}2}{4^k}\cdot\frac{(2k-2)!}{k!(k-1)!}$, we get that

$$f(x) = \sum_{k\geq 1}\frac{(2k-2)!}{k!(k-1)!}x^k = \sum_{k\geq 1}\frac{1}{k}\binom{2k-2}{k-1}x^k.$$

Note that $f(x)$ is the generating function of $\{b_k\}$, therefore

$$b_k = \frac{1}{k}\binom{2k-2}{k-1}.$$

This finishes the proof. ∎

1.9 Random Walks

Consider a real axis with integer points $(0, \pm 1, \pm 2, \pm 3, \cdots)$ marked. A frog leaps among the integer points according to the following rules:

(1). At beginning, it sits at 1.

(2). In each coming step, the frog leaps either by distance 2 to the right (from i to $i+2$), or by distance 1 to the left (from i to $i-1$), each of which is randomly chosen with probability $\frac{1}{2}$ independently of each other.

Problem 1.55. *What is the probability that the frog can reach "0"?*

Solution. In each step, we use "+" or "−" to indicate the choice of the frog that is either to leap right or leap left. Then the probability space Ω can be viewed as the set of infinite vectors, where each entry is in $\{+,-\}$.

Let A be the event that the frog reaches 0. Let A_i be the event that the frog reaches 0 at the i^{th} step for the first time. So $A = \cup_{i=1}^{+\infty}A_i$ is a disjoint union. So $P(A) = \sum_{i=1}^{+\infty}P(A_i)$.

To compute $P(A_i)$, we can define a_i to be the number of trajectories (or vectors) of the first i steps such that the frog starts at 1 and reaches 0 at the i^{th} step for the first time. So

$$P(A_i) = \frac{a_i}{2^i}.$$

Then,

$$P(A) = \sum_{i=1}^{+\infty}\frac{a_i}{2^i}.$$

Let $f(x) = \sum_{i=0}^{+\infty}a_ix^i$ be the generating function of $\{a_i\}_{i\geq 0}$, where $a_0 := 0$. Thus,

$$P(A) = \sum_{i=1}^{+\infty}\frac{a_i}{2^i} = f\left(\frac{1}{2}\right).$$

We then turn to find the expression of $f(x)$.

Let b_i be the number of trajectories of the first i steps such that the frog starts at "2" and reaches "0" at the i^{th} step for the first time.

Let c_i be the number of trajectories of the first i steps such that the frog starts at "3" and reaches "0" at the i^{th} step for the first time.

First we express b_i in terms of $\{a_j\}_{j\geq 1}$. Since the frog only can leap to left by distance 1, if the frog can successfully jump from "i" to "0" in i steps, then this frog must reach "1" first. Let j be the number of steps by which the frog reaches "1" for the first time. So there are a_j trajectories from "2" to "1" at the j^{th} step for the first time.in the remaining $i-j$ steps the frog must jump from "1" to "0" and reach "0" at the coming $(i-j)^{th}$ step for the first time, so there are a_{i-j} trajectories that the frog can finish in exactly $i-j$ steps. In total,

$$b_i = \sum_{j=1}^{i-1} a_j a_{i-j}.$$

As $a_j = 0$,

$$b_i = \sum_{j=0}^{i} a_j a_{i-j}.$$

We can get

$$\sum_{i\geq 0} b_i x^i = (\sum_{i\geq 0} a_i x^i)^2 = f^2(x).$$

Similarly, if we count the number c_i of trajectories from 3 to 0, we can obtain that

$$c_i = \sum_{j=0}^{i} a_j b_{i-j},$$

which implies that

$$\sum_{i\geq 0} c_i x^i = \left(\sum_{i\geq 0} b_i x^i\right)\left(\sum_{i\geq 0} a_i x^i\right) = f^3(x).$$

Let us consider a_i from another point of view. After the first step, either the frog reaches "0" directly (if it leaps to left, so $a_1 = 1$), or it leaps to "3". In the latter case, the frog needs to jump from "3" to "0" using $i-1$ steps. Thus for $i \geq 2$, $a_i = c_{i-1}$.

Combining the above facts, we have

$$f(x) = \sum_{i=0}^{+\infty} a_i x^i = x + \sum_{i\geq 2} a_i x^i = x + \sum_{i\geq 2} c_{i-1} x^i = x + x\left(\sum_{j=0}^{+\infty} c_j x^j\right) = x + x\cdot f^3(x).$$

Let $a := P(A) = f(1/2)$. Then $a = \frac{1}{2} + \frac{a^3}{2}$, i.e., $(a-1)(a^2+a-1) = 0$, implying that

$$a = 1,\ \frac{\sqrt{5}-1}{2},\ \text{or}\ \frac{-\sqrt{5}-1}{1}.$$

Since $P(A) \in [0,1]$, we see $P(A) = 1$ or $\frac{\sqrt{5}-1}{2}$.

Note that $f(x) = x + xf^3(x)$. Consider the inverse function of $f(x)$, that is, $g(x) := \frac{x}{1+x^3}$. Consider the figure of $g(x)$. We find that $g(x)$ is increasing around $\frac{\sqrt{5}-1}{2}$ but decreasing around 1. Since $f(x) = \sum a_i x^i$ is increasing, $g(x)$ also increases. Thus it doesn't make sense for $g(x)$ being around $x = 1$. This explains that $P(A) = \frac{\sqrt{5}-1}{2}$. ∎

1.10 Exponential Generating Functions

Let $\mathbb{N}, \mathbb{N}_e$ and $\mathbb{N}_o$ be the sets of non-negative integers, non-negative even integers and non-negative odd integers, respectively.

Given n sets I_j of non-negative integers for $j \in [n]$, let $f_j(x) = \sum_{i \in I_j} x^i$. Let a_k be the number of integer solutions to $i_1 + i_2 + ... + i_n = k$, where $i_j \in I_j$. Then $\prod_{j=1}^n f_j(x)$ is the ordinary generating function of $\{a_k\}_{k \geq 0}$.

Problem 1.56. *Let S_n be the number of selections of n letters chosen from an unlimited supply of a's, b's and c's such that both of the numbers of a's and b's are even.*

Solution. We can write S_n as

$$S_n = \sum_{e_1+e_2+e_3=n,\ e_1,e_2 \in \mathbb{N}_e,\ e_3 \in \mathbb{N}} 1.$$

Using the previous fact, we see that $S_n = [x^n]f$, where

$$f(x) = \left(\sum_{i \in \mathbb{N}_e} x^i\right)^2 \left(\sum_{j \in \mathbb{N}} x^j\right) = \left(\frac{1}{1-x^2}\right)^2 \cdot \frac{1}{1-x}.$$

∎

Problem 1.57. *Let T_n be the number of arrangements (or words) of n letters chosen from an unlimited supply of a's, b's and c's such that both of the numbers of a's and b's are even. What is the value of T_n?*

Solution. To solve this, we define a new kind of generating functions.

Definition 1.58. *The exponential generating function for the sequence $\{a_n\}_{n \geq 0}$ is the power series*

$$f(x) = \sum_{n=0}^{\infty} a_n \cdot \frac{x^n}{n!}.$$

Then we have the following fact.

Fact 1.59. *If we have n letters including x a's, y b's and z c's (i.e. $x + y + z = n$), then we can form $\frac{n!}{x!y!z!}$ distinct words using them.*

Therefore, a selection (say x a's, y b's and z c's) can contribute $\frac{n!}{x!y!z!}$ arrangements to T_n. This implies that

$$T_n = \sum_{e_1+e_2+e_3=n,\ e_1,e_2 \in \mathbb{N}_e,\ e_3 \in \mathbb{N}} \frac{n!}{e_1!e_2!e_3!}.$$

Similar to defining the above $f(x)$ for S_n, we define the following for T_n. Let

$$g(x) := \left(\sum_{i\in\mathbb{N}_e}\frac{x^i}{i!}\right)^2\left(\sum_{j\in\mathbb{N}}\frac{x^j}{j!}\right).$$

Claim. We have

$$[x^n]g = \frac{T_n}{n!}.$$

Proof. To see this, we expand $g(x)$. Then the term x^n in $g(x)$ becomes

$$\sum_{\substack{e_1+e_2+e_3=n,\\ e_1,e_2\in\mathbb{N}_e,\ e_3\in\mathbb{N}}}\frac{x^{e_1}}{e_1!}\cdot\frac{x^{e_2}}{e_2!}\cdot\frac{x^{e_3}}{e_3!} = \left(\sum_{\substack{e_1+e_2+e_3=n,\\ e_1,e_2\in\mathbb{N}_e,\ e_3\in\mathbb{N}}}\frac{n!}{e_1!e_2!e_3!}\right)\frac{x^n}{n!} = T_n\cdot\frac{x^n}{n!}.$$

So $[x^n]g = \frac{T_n}{n!}$, i.e., $g(x)$ is the exponential generating function of $\{T_n\}$. This finishes the proof of Claim. ∎

Using Taylor series: $e^x = \sum_{j\geq 0}\frac{x^j}{j!}$ and $e^{-x} = \sum_{j\geq 0}(-1)^j\frac{x^j}{j!}$, we have

$$\frac{e^x+e^{-x}}{2} = \sum_{j\in\mathbb{N}_e}\frac{x^j}{j!} \quad\text{and}\quad \frac{e^x-e^{-x}}{2} = \sum_{j\in\mathbb{N}_o}\frac{x^j}{j!}.$$

By the previous fact, we get

$$g(x) = \left(\frac{e^x+e^{-x}}{2}\right)^2\cdot e^x = \frac{e^{3x}+2e^x+e^{-x}}{4} = \sum_{n\geq 0}\left(\frac{3^n+2+(-1)^n}{4}\right)\cdot\frac{x^n}{n!}.$$

Therefore, we get that

$$T_n = \frac{3^n+2+(-1)^n}{4}.$$

∎

Recall that the *exponential generating function* for the sequence $\{a_n\}_{n\geq 0}$ is the power series

$$f(x) = \sum_{n=0}^{+\infty}a_n\cdot\frac{x^n}{n!}.$$

As we shall see, ordinary generation functions can be used to find the number of selections; while exponential generation functions can be used to find the number of arrangements or some combinatorial objects **involving ordering**. We summarize this as the following facts.

Fact 1.60. *Given $I_j\subseteq\mathbb{N}^+$ for $j\in[n]$, let $f_j(x) = \sum\limits_{i\in I_j}x^i$. And let $a_k = \sum\limits_{\substack{i_1+\ldots+i_n=k,\\ i_j\in I_j}}1$. Then*

$$\prod_{j=1}^{n}f_j(x) = \sum_{k=0}^{+\infty}a_kx^k.$$

Fact 1.61. *Given $I_j \subseteq \mathbb{N}^+$ for $j \in [n]$, let $g_j(x) = \sum\limits_{i \in I_j} \frac{x^i}{i!}$. And let $b_k = \sum\limits_{\substack{i_1+\ldots+i_n=k,\\ i_j \in I_j}} \frac{k!}{i_1!i_2!\ldots i_n!}$. Then*

$$\prod_{j=1}^{n} g_j(x) = \sum_{k=0}^{+\infty} \frac{b_k}{k!} x^k.$$

Fact 1.62. *Let $f(x) = \prod\limits_{j=1}^{n} f_j(x)$. Then*

$$[x^k]f = \sum_{\substack{i_1+\ldots+i_n=k,\\ i_j \geq 0}} \prod_{j=1}^{n} [x^{i_j}] f_j.$$

Fact 1.63. *Let $f(x) = \prod\limits_{j=1}^{n} f_j(x)$ and let $f_j(x) = \sum\limits_{k=0}^{+\infty} \frac{a_k^{(j)}}{k!} x^k$. Then*

$$f(x) = \sum_{k=0}^{+\infty} \frac{A_k}{k!} x^k,$$

if and only if

$$A_k = \sum_{\substack{i_1+\ldots+i_n=k,\\ i_j \geq 0}} \frac{k!}{i_1!i_2!\ldots i_n!} \Big(\prod_{j=1}^{n} a_{i_j}^{(j)} \Big).$$

Exercise 1.64. *Find the number a_n of ways to send n students to 4 different classrooms (say R_1, R_2, R_3, R_4) such that each room has at least 1 students.*

Solution.

$$a_n = \sum_{\substack{i_1+i_2+i_3+i_4=n,\\ i_j \geq 1}} \frac{n!}{i_1!i_2!i_3!i_4!}.$$

Let $I_j = \{1, 2, ...\}$ for $j \in [4]$ and $g_j(x) = \sum\limits_{i \geq 1} \frac{x^i}{i!} = e^x - 1$. By Fact 1.61, we have that

$$g_1 g_2 g_3 g_4 = \sum_{n=0}^{+\infty} \frac{a_n}{n!} x^n = (e^x - 1)^4 = e^{4x} - 4e^{3x} + 6e^{2x} - 4e^x + 1.$$

Thus $a_n = 4^n - 4 \cdot 3^n + 6 \cdot 2^n - 4$ for $n \geq 4$. ∎

Exercise 1.65. *Let a_n be the number of arrangements of type A for a group of n people, and let b_n be the number of arrangements of type B for a group of n people.*

Define a new arrangement of n people called type C as follows:

- *Divide the n people into 2 groups (say 1^{st} and 2^{nd}).*
- *Then arrange the 1^{st} group by an arrangement of type A, and arrange the 2^{nd} group by an arrangement of type B.*

Let c_n be the number of arrangements of type C of n people. Let $A(x), B(x), C(x)$ be the exponential generation function for $\{a_n\}, \{b_n\}, \{c_n\}$ respectively. Prove that $C(x) = A(x)B(x)$.

Proof. We can easily see that

$$c_n = \sum_{\substack{i+j=n, \\ i,j \geq 0}} \frac{n!}{i!j!} a_i b_j.$$

Then by Fact 1.63, $C(x) = A(x)B(x)$. ∎

2 Basic of Graphs

In this second part of our course, we will discuss many interesting results in graph theory. We first introduce several basic definitions about graphs.

Definition 2.1. *A graph $G = (V, E)$ consists of a vertex set V and an edge set E, where the elements of V are called vertices and the elements of $E \subseteq \binom{V}{2} = \{(x, y) : x, y \in V\}$ are called edges.*

- If E contains unordered pairs, then G is an undirected graph, otherwise G is a directed graph.
- In this course, all graphs are undirected and simple, i.e., it has NO loops or multiple edges.
- We say vertices x and y are adjacent if $(x, y) \in E$, write $x \sim_G y$ or $x \sim y$ or $xy \in E$.
- We say the edge xy is incident to the endpoints x and y.
- Let $e(G)$ be the number of edges in G, i.e., $e(G) = |E(G)|$.
- The degree of a vertex v in G, denoted by $d_G(v)$, is the number of edges in G incident to v.
- The neighborhood of a vertex v is the set of vertices u that is adjacent to v, i.e., $N_G(v) = \{u \in V(G) : u \sim v\}$. Thus we have $d_G(v) = |N_G(v)|$.
- A graph $G' = (V', E')$ is a subgraph of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E \cap \binom{V'}{2}$, i.e., $G' \subseteq G$.
- A subgraph $G' = (V', E')$ of $G = (V, E)$ is induced, if $E' = E \cap \binom{V'}{2}$.

Definition 2.2. *Two graphs $G = (V, E)$ and $G' = (V', E')$ are isomorphic if there exists a bijection $f : V \to V'$ such that $i \sim_G j$ if and only if $f(i) \sim_{G'} f(j)$.*

- A graph on n vertices is a complete graph (or a clique), denoted by K_n, if all pairs of vertices are adjacent. So we have $e(K_n) = \binom{n}{2}$.
- A graph on n vertices is called an independent set, denoted by I_n, if it contains no edges at all.
- Given a graph $G = (V, E)$, its complement is a graph $\overline{G} = (V, E^c)$ with $E^c = \binom{V}{2} \backslash E$.
- The degree sequence of a graph $G = (V, E)$ is a sequence of degrees of all vertices listed in a non-decreasing order.

• The path P_k of length $k-1$ is a graph $v_1v_2...v_k$ where $v_i \sim v_{i+1}$ for $i \in [k-1]$. Note that the length of a path P (denoted by $|P|$) is the number of *edges* in P.

• A cycle C_k of length k is a graph $v_1v_2...v_kv_1$ where $v_i \sim v_{i+1}$ for $i \in [k]$, where $v_{k+1} = v_1$.

• A graph G is planar, if we can draw G on the plane such that its intersects only at their endpoints.

Exercise 2.3. *Show that K_4 is planar but K_5 is not.*

The following Handshaking Lemma is the most basic lemma in graph theory.

Lemma 2.4 (Handshaking Lemma)**.** *In any graph $G = (V, E)$,*

$$\sum_{v \in V} d_G(v) = 2e(G).$$

Proof. Let $F = \{(e, v) : e \in E(G), v \in V(G) \text{ such that } v \text{ is adjacent to } e\}$. Then

$$\sum_{e \in E(G)} 2 = |F| = \sum_{v \in V} d_G(v).$$

∎

Corollary 2.5. *In any graph G, the number of vertices with odd degree is even.*

Proof. Let $O = \{v \in V(G) : d(v) \text{ is odd}\}$ and $\mathcal{E} = \{v \in V(G) : d(v) \text{ is even}\}$. Then by Lemma 2.4,

$$2e(G) = \sum_{v \in O} d_G(v) + \sum_{v \in \mathcal{E}} d_G(v).$$

Thus we have $\sum_{v \in O} d_G(v)$ is even, moreover we have $|O|$ is even. ∎

Corollary 2.6. *In any graph G, if there exists a vertex with odd degree, then there are at least two vertices with odd degree.*

3 Sperner's Lemma

Let us consider the following application of Corollary 2.6. First we draw a triangle in the plane, with 3 vertices $A_1A_2A_3$. Then we divide this triangle $\triangle = A_1A_2A_3$ into small triangles such that no triangle can have a vertex inside an edge of any other triangle. Then we assign 3 colors (say 1,2,3) to all vertices of these triangles, under the following rules.

(1) The vertex A_i is assigned by color i for $i \in [3]$.

(2) All vertices lying on the edge A_iA_j of the large triangle are assigned by the color i or j.

(3) All interior vertices are assigned by any color 1,2,3.

Lemma 3.1 (Sperner's Lemma (a planar version))**.** *For any assignment of colors described as above, there always exists a small triangle whose three vertices are assigned by three colors* $1, 2, 3$.

Proof. Define an auxiliary graph G as following.

- Its vertices are the faces of small triangles and the outer face. Let z be the vertex representing the outer face.

- Two vertices of G are adjacent, if the two corresponding faces are neighboring faces and the two endpoints of their common edge are colored by 1 and 2.

We consider the degree of any vertex $v \in V(G)\backslash\{z\}$.

(1) If the face of v has NO two endpoints with color 1 and 2, then $d_G(v) = 0$.

(2) If the face of v has 2 endpoints with color 1 and 2. Let k be the color of the third endpoint of this face. If $k \in \{1,2\}$, then $d_G(v) = 2$. Otherwise $k = 3$, then $d_G(v) = 1$ and this triangle has 3 colors 1,2,3.

Thus we have that $d_G(v)$ is odd if and only if $d_G(v) = 1$, and then the face of v has colors 1,2,3. Now we consider $d_G(z)$ and claim that it must be odd. Indeed, the edge of G incident to z obviously have to go across A_1A_2. Consider the sequence of the colors of the endpoints on A_1A_2, from A_1 to A_2. Then $d_G(z) =$ the number of alternations between 1 and 2 in this sequence, which must be odd. By Corollary 2.6, since the graph G has a vertex z with odd degree, there must be another vertex $v \in V(G)\backslash\{z\}$ with odd degree. Then $d(v) = 1$ and the face of v has colors 1,2,3. ∎

Theorem 3.2 (Brouwer's Fixed Point Theory in 2-dimension)**.** *Every continuous function $f : \triangle \to \triangle$ has a fixed point x, that is, $f(x) = x$.*

Proof. Consider a sequence of refinements of $\triangle$. Define three auxiliary functions $\beta_i : \triangle \to R$ for $i \in \{1,2,3\}$ as following:

For any $a = (x,y) \in \triangle$,

$$\begin{cases} \beta_1(a) & = x, \\ \beta_2(a) & = y, \\ \beta_3(a) & = 1 - x - y. \end{cases}$$

For any continuous $f : \triangle \to \triangle$, define $M_i = \{a \in \triangle : \beta_1(a) \geqslant \beta_1(f(a))\}$ for $i \in \{1,2,3\}$. Then we have the following facts.

(1) Any point $a \in \triangle$ belongs to at least one M_i.

(2) If $a \in M_1 \cap M_2 \cap M_3$, then a is a fixed point.

We want to define a coloring $\phi : \triangle \to \{1,2,3\}$ such that

(a) Any $a \in \triangle$ with $\phi(a) = i$ belongs to M_i.

(b) The coloring ϕ satisfies the conditions of Sperner's Lemma for any subdivision of $\triangle$.

Next we show such ϕ exists. This is because

- For the point A_i (say $i = 1$), we have that $A_1 = (1,0) \in M_1$, so we can let $\phi(A_i) = i$.

- Consider a vertex $a = (x,y) \in A_1A_2$, i.e., $x+y = 1$. Then $a \in M_1 \cup M_2$, otherwise $x+y < 1$ which is a contradiction. So we can color a by 1 or 2.

Now we define a sequence $\{\triangle_1, \triangle_2, ...\}$ of subdivisions of $\triangle$ such that the maximum diameter of small triangles in $\triangle_n$ is going to 0 as $n \to +\infty$. Applying Sperner's Lemma to each $\triangle_n$ and the coloring ϕ, we get that there exists a small triangle $A_1^{(n)} A_2^{(n)} A_3^{(n)}$ in $\triangle_n$ which has 3 colors 1,2,3.

Consider the sequence $\{A_1^{(n)}\}_{n\geq 1}$. Since everything is bound, there is a subsequence $\{A_1^{(n_k)}\}_{k\geq 1}$ such that $\lim\limits_{k\to+\infty} A_1^{(n_k)} = p \in \triangle$ exists. Since the diameter of $A_1^{(n)} A_2^{(n)} A_3^{(n)}$ is going to be 0 as $n \to +\infty$, we see that $\lim\limits_{k\to+\infty} A_2^{(n_k)} = \lim\limits_{k\to+\infty} A_3^{(n_k)} = p$. Since $\beta_i(A_i^{(n_k)}) \geqslant \beta_i(f(A_i^{(n_k)}))$ for $i \in [3]$ and f is continuous. We get $\beta_i(p) = \lim\limits_{k\to+\infty} \beta_i(A_i^{(n_k)}) \geq \lim\limits_{k\to+\infty} \beta_i(f(A_i^{(n_k)})) = \beta_i(f(p))$ for $i \in [3]$. This implies that $p \in M_1 \cap M_2 \cap M_3$, so p is a fixed point of f, i.e., $f(p) = p$. ∎

3.1 Double Counting

The basic setting of the double counting technique is as follows. Suppose that we are given two finite sets A and B, and a subset $S \subseteq A \times B$. If $(a, b) \in S$, then we say that a and b are incident. Let N_a be the number of elements $b \in B$ such that $(a, b) \in S$, and N_b be the number of elements $a \in A$ such that $(a, b) \in S$. Then we have

$$\sum_{a\in A} N_a = |S| = \sum_{b\in B} N_b.$$

Theorem 3.3. *Let $T(j)$ be the number of divisions of a positive integer j. Let $\overline{T(n)} = \frac{1}{n}\sum_{j=1}^{n} T(j)$. Then we have $|\overline{T(n)} - H(n)| < 1$, where $H(n) = \sum_{i=1}^{n} \frac{1}{i}$ is the n^{th} Harmonic number.*

Proof. Define a table $X = (x_{ij})$ where

$$x_{ij} = \begin{cases} 1 & if\ i|j \\ 0 & otherwise. \end{cases}$$

Then

$$\sum_{j=1}^{n} T(j) = \sum_{1\leq i\leq j\leq n} x_{ij} = \sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor,$$

which implies that

$$\overline{T(n)} = \frac{1}{n}\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor.$$

Then we have

$$|\overline{T(n)} - H(n)| < 1.$$

∎

Exercise 3.4. *Prove that*

$$\left| \frac{1}{n}\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor - \sum_{i=1}^{n} \frac{1}{i} \right| < 1.$$

3.2 Sperner's Theorem

Definition 3.5. *Let $\mathcal{F} \subseteq 2^{[n]}$ be a family of subsets of [n]. We say $\mathcal{F}$ is* <u>*independent*</u> *(or $\mathcal{F}$ is an independent system), if for any two $A, B \in \mathcal{F}$, we have $A \not\subset B$ and $B \not\subset A$. In other words, $\mathcal{F}$ is independent if and only if there is no "containment" relationship between any two subsets of $\mathcal{F}$.*

Fact 3.6. *For a fixed $k \in [n]$, $\binom{[n]}{k}$ is an independent system.*

Theorem 3.7 (Sperner's Theorem)**.** *For any independent system $\mathcal{F}$ of [n], we have*

$$|\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

First proof of Sperner's Theorem (Double-Counting). A *chain* of subsets of $[n]$ is a sequence of distinct subsets

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq ... \subseteq A_k.$$

A *maximal chain* is a chain with the property that no other subsets of $[n]$ can be inserted into it to find a longer chain. We have the following observations.

(1). Any maximal chain looks like:

$$\phi \subseteq \{x_1\} \subseteq \{x_1, x_2\} \subseteq ... \subseteq \{x_1, ..., x_k\} \subseteq ... \subseteq \{x_1, ..., x_n\}.$$

(2). There are exactly $n!$ maximal chains.

This is because any such a maximal chain, say $\mathcal{C} : \phi \subseteq \{x_1\} \subseteq \{x_1, x_2\} \subseteq ... \subseteq \{x_1, x_2, ..., x_n\}$, defines a unique permutation:

$$\pi : [n] \to [n], \pi(i) = x_i, \forall i \in [n].$$

Now we double counting the number of pairs $(\mathcal{C}, A)$ satisfying that:

- $\mathcal{C}$ is a maximal chain of $[n]$.
- $A \in \mathcal{C} \cap \mathcal{F}$.

Recall the rule of double counting given at the beginning that

$$\sum_{\mathcal{C}} N_{\mathcal{C}} = \text{the number of pairs } (\mathcal{C}, A) = \sum_{A} N_A,$$

where $N_{\mathcal{C}}$ is the number of subsets $A \in \mathcal{C} \cap \mathcal{F}$ and N_A is the number of maximal chains $\mathcal{C}$ contains A. It is key to observe that

- $N_{\mathcal{C}} \leq 1$,
- $N_A = |A|!(n - |A|)!$

So we have

$$n! = \sum_{\mathcal{C}} 1 \geq \sum_{\mathcal{C}} N_{\mathcal{C}} = \sum_{A\in\mathcal{F}} N_A = \sum_{A\in\mathcal{F}} |A|!(n-|A|)!$$
$$= \sum_{A\in\mathcal{F}} \frac{n!}{\binom{n}{|A|}} \geq \sum_{A\in\mathcal{F}} \frac{n!}{\binom{n}{\lfloor\frac{n}{2}\rfloor}} = \frac{n!}{\binom{n}{\lfloor\frac{n}{2}\rfloor}}|\mathcal{F}|,$$

which implies that

$$|\mathcal{F}| \leq \binom{n}{\lfloor\frac{n}{2}\rfloor}.$$

This finishes the proof.

∎

Now we give another proof of Sperner's Theorem.

Definition 3.8. *A chain is* <u>*symmetric*</u> *if it consists of subsets of sizes* $k, k+1, ..., \lfloor\frac{n}{2}\rfloor, ..., n-k-1, n-k$ *for some* $k \geq 0$.

For example, when $n = 3$, $\{\{2\},\{2,3\},\{1,2,3\}\}$ is not symmetric. And when $n = 4$, $\{\phi,\{1,2,3\}\}$ is not symmetric.

Theorem 3.9. *The family* $2^{[n]}$ *can be partitioned into a disjoint union of symmetric chains.*

Proof of Theorem 3.9. For each $A \in 2^{[n]}$, we define a sequence "$a_1a_2...a_n$" consisting of left and right parentheses by defining

$$a_i = \begin{cases} \text{“(”}, & \text{if } \quad i \in A \\ \text{“)”}, & \text{otherwise} \end{cases}$$

We then define the <u>"partial pairing of parentheses"</u> as following:

(1). First, we pair up all pairs "()" of adjoint parentheses.

(2). Then, we delete these already paired parentheses.

(3). Repeat the above process until nothing can be done.

Note that when this process stops, the remaining unpaired parentheses must look like this:

$$))))((((($$

We say two subsets $A, B \in 2^{[n]}$ have <u>the same partial pairing</u>, if the paired parentheses are the same (even in the same positions).

We can define an equivalence " $\sim$ " on $2^{[n]}$ by letting $A \sim B$ if and only if A, B have the same partial pairing.

Exercise 3.10. *Each equivalence class indeed forms a symmetric chain.*

Using this fact, now we see that $2^{[n]}$ can be partitioned into disjoint equivalence classes, which are disjoint symmetric chains. This finishes the proof. ∎

Theorem 3.9 can rapidly imply Sperner's Theorem.

Second proof of Sperner's Theorem. Note that by definition, any symmetric chain contains exactly one subset of size $\lfloor \frac{n}{2} \rfloor$. Since there are $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ many subsets of size $\lfloor \frac{n}{2} \rfloor$, by Theorem 3.9, we see that any partition of $2^{[n]}$ into symmetric chains has to consist of exactly $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ symmetric chains. Each symmetric chain can contain at most one subset from $|\mathcal{F}|$ and thus we see $|\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. ∎

3.3 Littlewood-Offord Problem

Theorem 3.11. *Fix a vector $\vec{a} = (a_1, a_2, ..., a_n)$ with each $|a_i| \geq 1$. Let $S = \{\vec{\epsilon} = (\epsilon_1, \epsilon_2, ..., \epsilon_n) : \epsilon_i \in \{1, -1\}$ and $\vec{\epsilon} \cdot \vec{a} \in (-1, 1)\}$, then $|S| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.*

Remark: Note that this is tight for many vectors $\vec{a}$.

Proof. For any $\vec{\epsilon} \in S$, define $A_{\vec{\epsilon}} = \{i \in [n] : a_i \epsilon_i > 0\}$. Let $\mathcal{F} = \{A_{\vec{\epsilon}} : \vec{\epsilon} \in S\}$. Then we have

$$|S| = |\mathcal{F}|.$$

Now we claim that $\mathcal{F}$ is an independent system. Suppose for a contradiction that there exist $A_{\vec{\epsilon}_1}, A_{\vec{\epsilon}_2} \in \mathcal{F}$ with $A_{\vec{\epsilon}_1} \subseteq A_{\vec{\epsilon}_2}$. That also says,

$$\begin{cases} \vec{\epsilon}_1 \cdot \vec{a} \in (-1, 1), \\ \vec{\epsilon}_2 \cdot \vec{a} \in (-1, 1), \end{cases}$$

which imply that

$$|\epsilon_1 \cdot \vec{a} - \epsilon_2 \cdot \vec{a}| < 2.$$

By definition, we have

$$\vec{\epsilon}_1 \cdot \vec{a} = \sum_{i \in A_{\vec{\epsilon}_1}} |a_i| - \sum_{i \notin A_{\vec{\epsilon}_1}} |a_i| = 2 \sum_{i \in A_{\vec{\epsilon}_1}} |a_i| - \sum_{i=1}^{n} |a_i|.$$

Since $A_{\vec{\epsilon}_1} \subseteq A_{\vec{\epsilon}_2}$, we also have that

$$\vec{\epsilon}_2 \cdot \vec{a} - \vec{\epsilon}_1 \cdot \vec{a} = 2(\sum_{i \in A_{\vec{\epsilon}_2}} |a_i| - \sum_{j \in A_{\vec{\epsilon}_1}} |a_j|) \geq 2|a_j| \geq 2, \text{ for some } j \in A_{\vec{\epsilon}_2} \setminus A_{\vec{\epsilon}_1},$$

a contradiction. By Sperner's Theorem, we have $|S| = |\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. This finishes the proof ∎

4 Turán Type Problem

Definition 4.1. *A graph G is bipartite if its vertex set can be partitioned into two parts (say A and B) such that each edge joints one vertex in A and another in B.*

This is equivalent to say that $V(G)$ can be partitioned into two independent subsets. And we say (A, B) is a bipartition of G. For example, all even cycles C_{2k} are bipartite, while all odd cycles C_{2k+1} are not.

Definition 4.2. *Let $K_{a,b}$ be the complete bipartite graph with two parts of sizes a and b. This is a bipartite graph with edge set $\{(i,j) : i \in A,\ j \in B\}$ where $|A| = a$ and $|B| = b$.*

Definition 4.3. *Given a graph H, we say a graph G is H-free if G dose not contain a copy of H as its subgraph.*

For example, $K_{a,b}$ is K_3-free.

Definition 4.4. *For fixed graph H, let the Turán number of H, denoted by $\mathrm{ex}(n, H)$, be the maximum number of edges in an n-vertex H-free graph G.*

Theorem 4.5. $\mathrm{ex}(n, C_4) \leqslant \dfrac{n}{4}(1 + \sqrt{4n-3})$.

Proof. Let G be a C_4-free graph with n vertices. We need to show that $e(G) \leqslant \dfrac{n}{4}(1 + \sqrt{4n-3})$. Consider $S = \{(\{u_1, u_2\}, w) : u_1wu_2$ is a path of length 2 in $G\}$. Since G is C_4-free, for fixed $\{u_1, u_2\}$, there is at most one vertex w such that $(\{u_1, u_2\}, w) \in S$. So we have

$$|S| = \sum_{\{u_1,u_2\}} \text{the number of } (\{u_1, u_2\}, w) \in S \leqslant \sum_{\{u_1,u_2\}} 1 = \binom{n}{2}.$$

On the other hand, fixed a vertex w, the number of $\{u_1, u_2\}$ such that $(\{u_1, u_2\}, w) \in S$ exactly equals $\binom{d(w)}{2}$, which implies that

$$|S| = \sum_{w \in V(G)} \binom{d(w)}{2} = \frac{1}{2} \sum_{w \in V(G)} d^2(w) - e(G).$$

Putting the above together, we have

$$\binom{n}{2} \geq |S| = \frac{1}{2} \sum_{w \in V(G)} d^2(w) - e(G).$$

Using Cauchy-Schwarz inequality, we have

$$\frac{n^2 - n}{2} \geq \frac{n}{2} \sum_{w \in V(G)} \frac{d^2(w)}{n} - e(G) \geq \frac{n}{2} \sum_{w \in V(G)} \left(\frac{d(w)}{n}\right)^2 - e(G),$$

which implies that

$$\frac{2e^2(G)}{n} - e(G) \leq \frac{n^2 - n}{2}.$$

Solving it, we can derive easily that $e(G) \leq \frac{n}{4}(1 + \sqrt{4n-3})$. ∎

Exercise 4.6. *Prove that* $\mathrm{ex}(n, C_4) < \frac{n}{4}(1 + \sqrt{4n-3})$.

Corollary 4.7. *We have* $\mathrm{ex}(n, C_4) \leqslant (\frac{1}{2} + o(n))n^{\frac{3}{2}}$*, where* $o(n) \to 0$ *as* $n \to \infty$.

Theorem 4.8 (Mantal's Thm)**.** $\mathrm{ex}(n, K_3) = \lfloor \frac{n^2}{4} \rfloor$.

Proof. We first consider the lower bound $\mathrm{ex}(n, K_3) \geqslant \lfloor \frac{n^2}{4} \rfloor$ as the complete bipartite graph $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$ is K_3-free and has $\lfloor \frac{n^2}{4} \rfloor$ edges.

Next, we show $\mathrm{ex}(n, K_3) \leqslant \lfloor \frac{n^2}{4} \rfloor$. We prove by induction on n that any n-vertex K_3-free graph G has at most $\frac{n^2}{4}$ edges. First it holds trivially when $n \in \{1, 2\}$. Now we assume that any K_3-free graph H with less than n vertices has at most $|V(H)|^2/4$ edges. Let G be K_3-free with n vertices. Take any edge of G, say $xy \in E(G)$. Since G is K_3-free, we say $N_G(x) \cap N_G(y) = \varnothing$, implies that $|d(x)| + |d(y)| \leqslant n$.

Let H be a graph obtained from G by deleting vertex x and y. Note that H is also K_3-free and has $n-2$ vertices. By induction, $e(H) \leqslant \frac{(n-2)^2}{4}$. Thus we have that

$$e(G) = e(H) + |d(x)| + |d(y)| - 1 \leqslant \frac{(n-2)^2}{4} + n - 1 = \frac{n^2}{4}.$$

This finishes the proof. ∎

Exercise 4.9. *The unique n-vertex K_3-graph which attains the maximum number of edges* $\mathrm{ex}(n, K_3)$ *is the complete bipartite graph $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$.*

5 Trees

Definition 5.1. *A graph G is connected, if for any vertices u and v, G contains a path from u to v. Otherwise, we say G is disconnected.*

Definition 5.2. *A component of a graph G is a maximal connected subgraph of G.*

Definition 5.3. *A graph T is called a tree if it is connected but contains no cycles. A vertex in a tree T with degree one is called a leaf.*

Fact 5.4 (Euler's Formula on trees)**.** *For any tree $T = (V, E)$, we have $|V| = |E| + 1$.*

Proof. First, any tree has at least one leaf. As otherwise, all vertices have degree at least 2, then this gives a cycle, a contradiction.

Next we apply induction on n. Consider the base case that $n = 2$, the tree is an edge, then we are done. Now we assume the statement holds for any tree on $n-1$ vertices. Consider a tree T on n vertices ($n \geq 2$). We know that T contains a leaf, call v. It is easy to see that $T - \{v\}$ is still a tree as it is connected and has no cycles which has $n-1$ vertices. By induction, $T - \{v\}$ has $n-2$ edges. So T has $n-1$ edges. ∎

Fact 5.5. *Any tree T with at least 2 vertices has at least 2 leaves.*

Proof. Assume for a contradiction that an n-vertex tree T has exactly one leaf v, then $d(u) \geq 2$ for any $u \in V(T) \backslash \{v\}$. Thus

$$2(n-1) = 2e(T) = \sum_{x \in V(T)} d(x) \geq 2(n-1) + 1 = 2n - 1,$$

a contradiction. ∎

Theorem 5.6 (Tree characterization)**.** *Let $T = (V, E)$ be a graph. Then the following are equivalent:*

(i). T is a tree (i.e. connected and no cycle.)

(ii). T is a "minimal" connected graph. (i.e. deleting any edge will result in a disconnected graph.)

(iii). T is a "maximal" graph without a cycle. (i.e. adding any new edge will result in a cycle.)

Proof. (i)⇒(ii): Suppose (ii) fails, then there exists $e = xy \in E(T)$ such that $T - \{e\}$ is still connected. Then $T - \{e\}$ has a path P from x to y. So $P \cup \{e\}$ is a cycle in T, a contradiction.

(ii)⇒(i): Suppose (i) fails, then T contains a cycle C. If we delete any edge e from C, $T - \{e\}$ remains connected, a contradiction.

(i)⇒(iii): For any new edge $e = xy$, as T is connected, T has a path P from x to y. Thus, $P \cup \{e\}$ gives a cycle.

(iii)⇒(i): Suppose (i) fails, so T is disconnected. Then T has two components, say D_1 and D_2. Pick $x \in D_1$ and $y \in D_2$. If we add the new edge $e = xy$, then it is easy to see that $T + \{e\}$ still has no cycle, a contradiction. ∎

Definition 5.7. *Given a graph G, a subgraph H of G is a spanning subgraph if $V(H) = V(G)$.*

Fact 5.8. *Any graph G is connected if and only if it contains a spanning tree.*

Proof. If G has a spanning tree then it is connected.

Suppose G is connected. Deleting edges of G until it satisfies the property (ii) in the theorem-5.6, then we get a spanning tree. ∎

Definition 5.9. *Given a connected graph G with n vertices, say $v_1, ..., v_n$. Let $ST(G)$ be the number of labeled spanning trees in G.*

Theorem 5.10 (Cayley's Formula)**.** *For an integer $n \geq 2$,*

$$ST(K_n) = n^{n-2}.$$

We will give 3 proofs for this formula.

5.1 The First Proof of Cayley's Formula

Let $V(K_n) = \{v_1, v_2, \cdots, v_n\}$ and given a spanning tree T. Then

$$\sum_{i=1}^{n} d(v_i) = 2e(T) = 2n - 2.$$

Now we introduce a lemma.

Lemma 5.11. *Let $d_1, d_2, ..., d_n$ be positive integers with $\sum_{i=1}^{n} d_i = 2n - 2$. Then the number of spanning trees in K_n on vertex set $\{v_1, ..., v_n\}$ satisfying $d(v_i) = d_i$ is equal to*

$$\frac{(n-2)!}{(d_1 - 1)!(d_2 - 1)! \cdots (d_n - 1)!}.$$

Proof. We prove by induction on n. Base case is trivial. When $n = 2$, $d_1 = d_2 = 1$. There is only one spanning tree.

Now we assume that this statement holds for any sequence of $n-1$ positive integers. Then consider $d_1, ..., d_n$ with $\sum_{i\in[n]} d_i = 2n-2$. By average, $(\sum d_i)/n < 2$, so there exists some $d_i = 1$, say $d_n = 1$. Let $\mathcal{F}$ be the family of all spanning trees with $d(v_i) = d_i$ for $i \in [n]$. And let $\mathcal{F}_i = \{T - \{v_n\} : T \in \mathcal{F}$, the unique neighbor of v_n in T is $v_i\}$. So $|\mathcal{F}| = \sum_{i=1}^{n-1} |\mathcal{F}_i|$. All trees in $\mathcal{F}_i$ have $n-1$ vertices $\{v_1, v_2, \cdots, v_{n-1}\}$ such that

$$\begin{cases} d(v_j) = d_j, & j \neq i, \\ d(v_i) = d_i - 1, & \text{otherwise.} \end{cases}$$

By induction, we have

$$|\mathcal{F}_i| = \frac{(n-3)!}{(d_1-1)!\cdots(d_i-2)!\cdots(d_{n-1}-1)!} = \frac{(n-3)!(d_i-1)}{\prod_{j=1}^{n-1}(d_j-1)!}.$$

So

$$|\mathcal{F}| = \sum_{i=1}^{n-1} |\mathcal{F}_i| = \frac{(n-3)!}{\prod_{j=1}^{n-1}(d_j-1)!}\left(\sum_{i=1}^{n-1}(d_i-1)\right) = \frac{(n-2)!}{\prod_{j=1}^{n}(d_j-1)!}.$$

∎

Recall the multinomial Theorem:

$$(x_1 + x_2 + \cdots x_k)^n = \sum_{i_1+\cdots i_k=n} \frac{n!}{i_1!\cdots i_k!} x_1^{i_1}\cdots x_k^{i_k},$$

which implies

$$k^n = \sum_{i_1+\cdots i_k=n} \frac{n!}{i_1!\cdots i_k!}.$$

Thus we have

$$ST(K_n) = \sum_{\substack{\sum_{i=1}^n d_i = 2n-2 \\ d_i \geq 1}} \frac{(n-2)!}{\prod_{j=1}^{n}(d_j-1)!} = n^{n-2}.$$

5.2 The Second Proof of Cayley's Formula

Definition 5.12. *A digraph $D = (V, A)$ consists of a vertex set V and an arc set $A \subseteq \{(i, j) : i, j \in V\}$*

Let $\mathscr{D}$ be the family of digraphs $D = ([n], A)$ such that each vertex in D has exactly one arc going out (i.e. each vertex has out degree one).

Fact 5.13.

$$|\mathscr{D}| = n^n.$$

Proof. Consider the set $\mathscr{F} = \{\text{all mapping } f : [n] \to [n]\}$. It is easy to see there exists a bijection between $\mathscr{D}$ and $\mathscr{F}$. So $|\mathscr{D}| = |\mathscr{F}| = n^n$. ∎

Definition 5.14. *Given a spanning tree of K_n, we choose 2 special vertices (one marked by a circle and the other marked by a square; these two vertices can be the same vertex). We call such a subject (the spanning tree with 2 special vertices) as a* <u>*vertebrate*</u>.

Let $\mathscr{V}$ be a family of all vertebrates on $[n]$. Clearly, $|\mathscr{V}| = ST(K_n)n^2$. So to get the Cayley's formula, it suffices to show $|\mathscr{V}| = n^n$.

Lemma 5.15. *There exists a bijection between $\mathscr{V}$ and $\mathscr{D}$.*

Proof. Consider a $W \in \mathscr{V}$ (see figure 1). Let P be the unique path in W between the two special vertices (marked by a circle and a square); and view P as a directed path from the circle to the square.

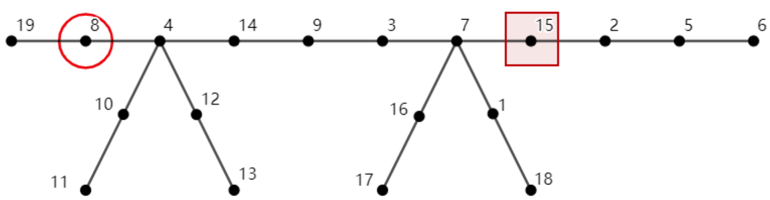


Figure 1: A vertebrate

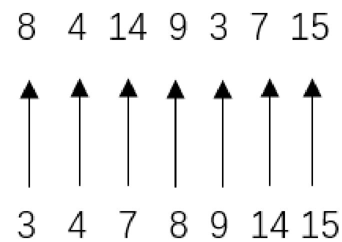


Figure 2: D_1

We then define a digraph D_1 on $V(P)$ by assign the following arcs (figure 2): that is, we place two rows, where the 1^{st} row is from P and the 2^{nd} row is the increasing sequence of $V(P)$, then we orient the arcs of D_1 from the vertices of the 2^{nd} row to the one above it. Thus each vertex in D_1 has exactly one arc out and one arc going in.

Exercise 5.16. *D_1 consists of vertex-disjoint directed cycle. (possibly loops and 2-cycles)*

Next, we extend D_1 to a digraph D on $[n]$, by the following:

(1) We remove all edges of P from W.

(2) Then $W - E(P)$ consists of subtrees, each having one vertex from $V(P)$. We direct the edges of these subtrees such that they point to the unique vertex of the component contained in $V(P)$.

(3) There arcs product in (2) together with the arcs of D_1, define a new graph D_W on $[n]$. This should be easy to see that $D_W \in \mathscr{D}$.

So we just define a mapping $\varphi : \mathscr{V} \to \mathscr{D}$, by assigning $\varphi(W) = D_W$, $W \in \mathscr{D}$. Next, We show φ is a bijection.

Step 1. We can define $\varphi^{-1} : \mathscr{D} \to \mathscr{V}$ such that $\varphi^{-1} \cdot \varphi = Id$.

Remark: In any D_W, $V(D_1)$ consists of all vertices in D_W contained in a directed cycle.

Take any $D \in \mathscr{D}$, there exists some vertex of D contained in a directed cycle. Let X be the set of all such vertices of D. Since $D[X]$ consists of vertex-disjoint directed cycles, there is a nature way to define a path as following (see figure 3):

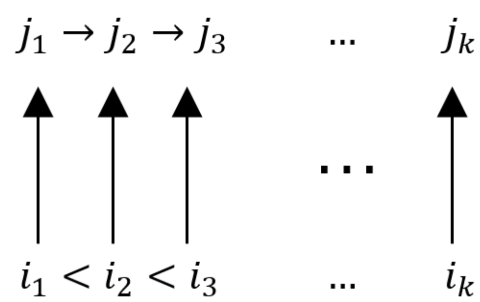


Figure 3: Define a path

First, list the vertices of X in the increasing order. Second, list the out-neighbor vertices of X in another row, respectively. Then the second row defines a path P be the special path in the vertebrate. Then it is easy to define the rest part of the vertebrate say W. So we have $D \in \mathscr{D} \xrightarrow{\varphi^{-1}} W \in \mathscr{V}$. We can check that $\varphi^{-1} \cdot \varphi = Id$.

Step 2. φ is a surjective.

We have proved in Step 1 that for any $D \in \mathscr{D}$, there exists $W \in \mathscr{V}$ satisfying $\varphi(W) = D$.

Therefore indeed φ is a bijection. ∎

Combining Fact 5.13 with Lemma 5.15, we get $ST(K_n) = n^{n-2}$.

5.3 The Third Proof of Cayley's Formula

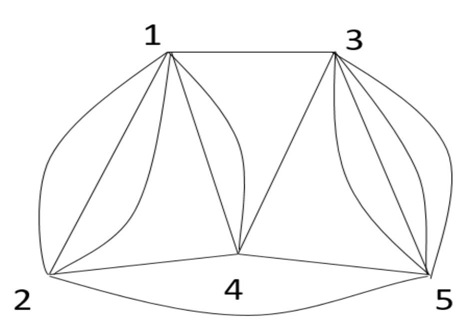
Definition 5.17. *A multigraph is a graph, where we allow multiple edges between vertices but do not allow loops.*

For a multigraph G in $[n]$, we define the Laplace matrix $Q = (q_{ij})_{n \times n}$ of G as follows:

$$q_{ij} = \begin{cases} d_G(i), & \text{if } i = j. \\ -m, & \text{if } i \neq j \text{ and there are } m \text{ edges between } i \text{ and } j. \end{cases}$$

Note that Q is symmetric, and the sum of each row/column is 0.

For example



$$Q = \begin{pmatrix} 6 & -3 & -1 & -2 & 0 \\ -3 & 5 & 0 & -1 & -1 \\ -1 & 0 & 6 & -1 & -4 \\ -2 & -1 & -1 & 5 & -1 \\ 0 & -1 & -4 & -1 & 6 \end{pmatrix}.$$

For an $n \times n$ matrix Q, let Q_{ij} be the $(n-1) \times (n-1)$ matrix obtained from Q by deleting the i^{th} row and j^{th} column.

Theorem 5.18. *For any multigraph G, $ST(G) = det(Q_{11})$, where Q_{ij} is the $(n-1) \times (n-1)$ matrix obtained from the Laplace matrix Q of G by deleting the i^{th} row and j^{th} column.*

Proof. We prove this by using induction on the number of edges in G. Base case, suppose that $e(G) = 1$. Then it holds trivially.

Now we consider a multigraph G and assume this holds for any multigraph with less than $e(G)$ edges. Take any edge e in G. Define two multigraph as following.

1. $G - e =$ the multigraph obtained from G be deleting the edge e.
2. $G/e =$ the multigraph obtained from G by contracting the two endpoints x, y of e into a new vertex z and adding new edges in $\{zu : xu \in E(G)\} \cup \{zu : yu \in E(G)\}$.

Let Q' and Q'' be the Laplace matrices of $G - e$ and G/e respectively. If in a multigraph G the vertex number 1 is not incident to any edge, then we have $T(G) = 0$. The first row of the Laplace matrix consists only of zeros, the sum of the rows of Q_{11} is also zero. Thus, $det(Q_{11}) = 0$. If the vertex number 1 is incident to at least one edge. More precisely, assume that the edge e has endpoints 1 and 2. So

$$Q' = \begin{pmatrix} 5 & -2 & -1 & -2 & 0 \\ -2 & 4 & 0 & -1 & -1 \\ -1 & 0 & 6 & -1 & -4 \\ -2 & -1 & -1 & 5 & -1 \\ 0 & -1 & -4 & -1 & 6 \end{pmatrix}, Q'' = \begin{pmatrix} 5 & -1 & -3 & -1 \\ -1 & 6 & -1 & -4 \\ -3 & -1 & 5 & -1 \\ -1 & -4 & -1 & 6 \end{pmatrix}.$$

Let $Q_{11,22}$ be the matrix obtained from Q by deleting the first two rows and the first two columns. Then we have

$$det(Q_{11}) = det((Q')_{11}) + det(Q_{11,22}). \tag{5.2}$$

We also see that

$$Q_{11,22} = (Q'')_{11}. \tag{5.3}$$

By (5.2) and (5.3) we have

$$det(Q_{11}) = det((Q')_{11}) + det((Q'')_{11}). \tag{5.4}$$

Claim. For any edge e in G, we have

$$ST(G) = ST(G - e) + ST(G/e). \tag{5.5}$$

Proof. We divide the spanning trees of G into two classes:

-the 1^{st} class contains those spanning trees of G NOT containing e, which are exactly $ST(G-e)$.

-the 2^{nd} class contains those spanning trees of G containing e. We can easily see that the trees in the 2^{nd} class are one-to-one corresponding to the spanning trees of G/e.

This proves (5.5). ∎

By induction, we have $ST(G-e) = det(Q'_{11})$, $ST(G/e) = det((Q'')_{11})$. By (5.4), we have $ST(G) = det(Q_{11})$. ∎

For K_n, we have

$$Q = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix}_{n\times n},$$

which implies that $ST(G) = det(Q_{11}) = n^{n-2}$.

6 Intersecting Family

Definition 6.1. *A family $\mathcal{F} \subset 2^{[n]}$ is intersecting if for any $A, B \in \mathcal{F}$, we have $A \bigcap B \neq \emptyset$.*

Fact 6.2. *For any intersecting family $\mathcal{F} \subset 2^{[n]}$, we have $|\mathcal{F}| \leq 2^{n-1}$.*

Proof. Consider all pairs $\{A, A^c\}$ for all $A \subset [n]$. Note that there are exactly 2^{n-1} such pairs, and $\mathcal{F}$ can have at most one subset from every pairs. This proves $|\mathcal{F}| \leq 2^{n-1}$. ∎

Note that this is tight:

- $\mathcal{F} = \{A \subset [n] : 1 \in A\}$.
- For n is odd, $\mathcal{F} = \{A \in [n] : |A| > \frac{n}{2}\}$.

A harder problem: What is the largest intersecting family $\mathcal{F} \subset \binom{[n]}{k}$, for fixed k?

Theorem 6.3 (Erdős-Ko-Rado Theorem)**.** *For $n \geq 2k$, the largest intersecting family $\mathcal{F} \subset \binom{[n]}{k}$ has size $\binom{n-1}{k-1}$.*

Moreover, if $n > 2k$, then the largest intersecting family $\mathcal{F} \subset \binom{[n]}{k}$ must be $\mathcal{F} = \{A \in \binom{[n]}{k} : t \in A\}$ for some fixed $t \in [n]$.

Proof. Take a cyclic permutation $\pi = (a_1, a_2, ..., a_n)$ of $[n]$. Note that there are $(n-1)!$ cyclic permutations of $[n]$ in total.

Let $\mathcal{F}_\pi = \{A \in \mathcal{F}$: A appears as k consecutive numbers in the circuit of π.$\}$

Claim 1. For all cyclic permutation π, assume $n \geq 2k$, then $|\mathcal{F}_\pi| \leq k$.

Proof. Pick $A \in \mathcal{F}_\pi$, say $A = \{a_1, a_2, ..., a_k\}$. We call the edges $a_n a_1, a_k a_{k+1}$ as the boundary edges of A, and the edges $a_1a_2, a_2a_3, ..., a_{k-1}a_k$ as the inner-edges of A. We observe that for any distinct $A, B \in \mathcal{F}_\pi$, the boundary-edges of A and B are distinct. For any $B \in \mathcal{F}_\pi \setminus \{A\}$, as $A \bigcap B \neq \phi$. we see that one of the boundary-edges of B must be an inner-edge of A. But A has $k-1$ inner-edges, so we see that there are at most $k-1$ many subsets in $\mathcal{F}_\pi \setminus \{A\}$. So $|\mathcal{F}_\pi| \leq k$. ∎

Next we do a double-counting. Let N be the number of pairs (π, A), where π is a cyclic permutation of [n], and $A \in \mathcal{F}_\pi$. By Claim 1, $N = \sum_\pi |\mathcal{F}_\pi| \leq k(n-1)!$. Fix A, how many cyclic π such that $A \in \mathcal{F}_\pi$? The answer is $k!(n-k)!$. So the number of cyclic permutations π such that π contains the elements of A as k consecutive numbers is $k!(n-k)!$. So we have

$$k(n-1)! \geq N = \sum_{A \in \mathcal{F}} k!(n-k)! = |\mathcal{F}|k!(n-k)!,$$

which implies that

$$|\mathcal{F}| \leq \frac{k \cdot (n-1)!}{k!(n-k)!} = \binom{n-1}{k-1}.$$

If $n > 2k$, for the extremal case $\mathcal{F} = \binom{n-1}{k-1}$, we want to show $\mathcal{F}$ must be a star. From the preview proof, we see that for any cycle permutation π, $|\mathcal{F}_\pi| = k$. And we have following claim.

Claim 2. Fix any $\pi = (a_0, a_1, ..., a_{n-1})$. If $\mathcal{F}_\pi = \{A_1, A_2, ..., A_k\}$, then $A_1 \cap A_2 \cap ... \cap A_k = \{t\}$ for some $0 \leq t \leq n-1$, where $A_j = \{a_{j+r}, a_{j+r+1}, ..., a_{j+r+k-1}\}$ for $1 \leqslant j \leqslant k$ and for some $0 \leq r \leq n-1$ (where the indices are taken under the additive group $\mathbb{Z}_n$.) .

Proof. With loss of generality, suppose that $A = \{a_1, ...a_k\} \in \mathcal{F}_\pi$. From the preview proof, we know a_ia_{i+1} is boundary-edge of some $B_i \in \mathcal{F}_\pi$ where $i \in [k-1]$, and for any distinct $A, B \in \mathcal{F}_\pi$, the boundary-edges of A and B are distinct. For any $B \in \mathcal{F}$, we color the two boundary-edges by 1 and 0, respectively, according to the clockwise direction. Since a_0a_1 has color 1 and a_ka_{k+1} has color 0. There must exist $\ell \in [k]$ such that $a_{\ell-1}a_\ell$ has color 1 and $a_\ell a_{\ell+1}$ has color 0. Let $A_1 = \{a_{\ell-k+1}, a_{\ell-k+2}, ..., a_{\ell-1}, a_\ell\}$ and $A_k = \{a_\ell, a_{\ell+1}, ..., a_{\ell+k-1}\}$. Since $\mathcal{F}$ is intersecting and $n > 2k$, there dose not exist j such that $a_{j-1}a_j$ has color 0 and a_ja_{j+1} has color 1. Then $a_{\ell-1+i}, a_{\ell+i}$ has color 0 for every $i \in [k]$. This finishes the proof. ∎

Fix π, let $\mathcal{F}_\pi = \{A_1, A_2, ..., A_k\}$ and let $A_1 \cap A_2 \cap ... \cap A_k = \{t\}$. If any element of $\mathcal{F}$ contains t, then $\mathcal{F}$ is a star, we are done. So we may assume that there exists $A_0 \in \mathcal{F}$ such that $t \notin A_0$.

Claim 3. For any $B \in \binom{A_1 \cup A_k \setminus \{t\}}{k-1}$, we have $B \cup \{t\} \in \mathcal{F}$.

Proof of Claim 3. Consider another cycle permutation π' with A_1, A_k unchanged, but the order of the integers inside $A_1 \setminus \{t\}$ and $A_k \setminus \{t\}$ are changed.

Since $A_1, A_k \in \mathcal{F}_{\pi'}$, by Claim 2 all other k-sets in $A_1 \cup A_k$ formed by k consecutive integers on π' are also in $\mathcal{F}_{\pi'} \subseteq \mathcal{F}$. Repeating using the argument, we prove Claim 3. ∎

Claim 4. The subset $A_0 \in \mathcal{F}$ (with $t \notin A_0$) satisfies $A_0 \subseteq A_1 \cup A_k \setminus \{t\}$.

Proof of Claim 4. Otherwise, A_0 has at most $k-1$ elements in $A_1 \cup A_k$. Then we have $|A_1 \cup A_k - A_0| \geqslant k$ (as $|A_1 \cup A_k| = 2k-1$). So, we can pick a k-subset $B \subseteq A_1 \cup A_k - A_0$ such that $t \in B$. By Claim 3, we have $B \in \mathcal{F}$. But $A_0 \cap B = \emptyset$, contradicting that $\mathcal{F}$ is intersecting. This proves Claim 4. ∎

Claim 5. We have $\binom{A_1 \cup A_k}{k} \subseteq \mathcal{F}$.

Proof of Claim 5. Consider any $i \in A_0$, let $B_i = (A_1 \cup A_k \setminus A_0) \cup \{i\}$. Since $t \in B_i$, by Claim 3, we have $B_i \in \mathcal{F}$. Repeating the proof of Claim 3, we can obtain that any k-subset of $A_1 \cup A_k$ containing i belongs to $\mathcal{F}$. In other words, any k-subset B of $A_1 \cup A_k$ must intersect A_0, and thus belongs to $\mathcal{F}$. Then we have $\binom{A_1 \cup A_k}{k} \subseteq \mathcal{F}$. ∎

If there exists a k-subset $C \in \mathcal{F}$ such that $B \nsubseteq A_1 \cup A_k$, then $|A_1 \cup A_k - B| \geqslant k$. So there exists $D \subseteq A_1 \cup A_k - C$ with $|D| = k$. By Claim 5, we have $D \in \mathcal{F}$, but $C \cap D = \emptyset$, a contradiction. This proves $\binom{A_1 \cup A_k}{k} = \mathcal{F}$.

Since $n > 2k$, we see $|\mathcal{F}| = \binom{2k-1}{k} = \binom{2k-1}{k-1} < \binom{n-1}{k-1} = |\mathcal{F}|$, a contradiction. This completes the proof.

∎

6.1 The Second Proof of Erdős-Ko-Rado Theorem

Definition 6.4. *A Kneser graph $K(n,k)$ with $n \geqslant 2k$ is a graph with vertex set $\binom{[n]}{k}$ such that for any two sets $A, B \in \binom{[n]}{k}$, A is adjacent to B in $K(n,k)$ if and only if $A \cap B = \varnothing$.*

One can easily check that $K(5,2)$ is the Petersen graph.

Definition 6.5. *Given a graph G, we let $\alpha(G)$ be the number of vertices in a largest independent set in G.*

We note that any independent set in $K(n,k)$ is an intersecting family in $\binom{[n]}{k}$. Therefore, we have the following.

Theorem 6.6 (Erdős-Ko-Rado (Restatement))**.** *For $n \geq 2k$, $\alpha(K(n,k)) \leqslant \binom{n-1}{k-1}$.*

Definition 6.7. *The adjacency matrix $A_G = (a_{ij})_{n \times n}$ of an n-vertex graph G is defined by*

$$a_{ij} = \begin{cases} 1, & \text{if } ij \in E(G), \\ 0, & \text{otherwise.} \end{cases}$$

Definition 6.8. *The eigenvalues $\lambda_1 \geqslant \lambda_2 \geqslant ... \geqslant \lambda_n$ of A_G is called the eigenvalues of G. The eigenvectors $\vec{v}_1, \vec{v}_2, ..., \vec{v}_n$ of A_G satisfying*

$$\begin{cases} A_G \vec{v}_i = \lambda_i \vec{v}_i, \\ ||\vec{v}_i|| = 1, \\ \vec{v}_i \perp \vec{v}_j \quad \text{for any } i \neq j, \end{cases}$$

are called the orthonormal eigenvectors of G.

Note that A_G is an $n \times n$ 0/1 symmetric matrix. Thus all the eigenvalues of G are real numbers.

Definition 6.9. *A graph G is d-regular if all vertices have the same degree d.*

Exercise 6.10. *If G is d-regular, then the largest eigenvalue of G is d.*

Theorem 6.11 (Hoffman's Theorem)**.** *If an n-vertex graph G is d-regular with eigenvalues $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$, then $\alpha(G) \leqslant n \cdot \dfrac{-\lambda_n}{\lambda_1 - \lambda_n}$*

Proof. Let $V(G) = [n]$. Let $\vec{v}_1, \ldots, \vec{v}_n$ be the corresponding orthonormal eigenvectors of eigenvalues $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$ of G. Thus we have

$$\begin{cases} A_G \vec{v}_i = \lambda_i \vec{v}_i, \\ ||\vec{v}_i|| = 1, \\ \vec{v}_i \perp \vec{v}_j, \text{ i.e., } < \vec{v}_i, \vec{v}_j >= 0, \text{ for any } i \neq j. \end{cases}$$

Let I be an independent set of G with $|I| = \alpha(G)$. Let $\vec{1}_I \in \{0,1\}^n$ be the vector such that its j^{th} coordinate is 1 if $j \in I$, and 0 otherwise. Then we can write

$$\vec{1}_I = \sum_{i=1}^{n} \alpha_i \vec{v}_i \text{ for some } \alpha_i \in \mathbb{R}.$$

Then we have

$$|I| =< \vec{1}_I, \vec{1}_I >=< \sum_i \alpha_i \vec{v}_i, \sum_j \alpha_j \vec{v}_j >= \sum_{i=1}^{n} \alpha_i^2, \tag{6.6}$$

where $\alpha_i =< \vec{1}_I, \vec{v}_i >$.

Since G is d-regular, we have that $\lambda_1 = d$ and $\vec{v}_1 = (1/\sqrt{n}, \ldots, 1/\sqrt{n})^T$. So we get

$$\alpha_1 =< \vec{1}_I, \vec{v}_1 >= \frac{|I|}{\sqrt{n}}. \tag{6.7}$$

Since I is an independent set in G,

$$\vec{1}_I^T A_G \vec{1}_I = \sum_{i,j} (\vec{1}_I)_i a_{ij} (\vec{1}_I)_j = 0,$$

where $A(G) = (a_{ij})$. On the other hand, we also have

$$\begin{aligned} 0 = \vec{1}_I^T A_G \vec{1}_I &= \big(\sum_i \alpha_i \vec{v}_i\big)^T A_G \big(\sum_j \alpha_j \vec{v}_j\big) = \big(\sum_i \alpha_i \vec{v}_i\big)^T \big(\sum_j \alpha_j \lambda_j \vec{v}_j\big) \\ &= \sum_{i=1}^{n} \alpha_i^2 \lambda_i \geq \alpha_1^2 \lambda_1 + (\alpha_2^2 + \cdots + \alpha_n^2) \lambda_n \overset{\text{by (6.6) (6.7)}}{=} \frac{|I|^2}{n} \lambda_1 + \left(|I| - \frac{|I|^2}{n}\right) \lambda_n. \end{aligned}$$

Thus we have

$$\frac{|I|^2}{n} \lambda_1 + \left(|I| - \frac{|I|^2}{n}\right) \lambda_n \leq 0, \quad \text{and} \quad |I| \left(\frac{|I|}{n} \lambda_1 + \lambda_n - \frac{|I|}{n} \lambda_n\right) \leq 0,$$

which implies that

$$\alpha(G) = |I| \leq n \cdot \frac{-\lambda_n}{\lambda_1 - \lambda_n}.$$

∎

Theorem 6.12 (see GTM 207, Theorem 9.4.3)**.** *The eigenvalues of Kneser graph $K(n,k)$ are:*

$$u_j = (-1)^j \binom{n-k-j}{k-j} \text{ of multiplicity } \binom{n}{j} - \binom{n}{j-1}$$

for every $0 \le j \le k$.

Proof of Theorem 6.6. Consider the eigenvalues of $K(n,k)$, say $\lambda_1 \ge \lambda_2 \cdots \ge \lambda_{\binom{n}{k}}$, where $\lambda_1 = \binom{n-k}{k}$, $\lambda_{\binom{n}{k}} = -\binom{n-k-1}{k-1}$. By Hoffman's bound,

$$\alpha(K(n,k)) \le \binom{n}{k} \frac{-\lambda_{\binom{n}{k}}}{\lambda_1 - \lambda_{\binom{n}{k}}} = \binom{n}{k} \frac{\binom{n-k-1}{k-1}}{\binom{n-k}{k} + \binom{n-k-1}{k-1}} = \binom{n-1}{k-1},$$

as desired. ∎

7 Partially Ordered Sets (Poset)

7.1 Poset

Let X be a finite set.

Definition 7.1. *R is a relation on X, if $R \subseteq X \times X$ where $X \times X$ denote the Cartesion product of X, i.e., $X \times X = \{(x_1, x_2) : \forall x_1, x_2 \in X\}$. If $(x, y) \in R$, then we often write xRy.*

Definition 7.2. *A partially ordered set (poset for short) is an ordered pair (X, R), where X is a finite set and R is a relation on X such that the following hold:*

(1) R is reflective: xRx for any $x \in X$,

(2) R is antisymmetric: if xRy and yRx, then $x = y$,

(3) R is transitive: if xRy and yRz, then xRz.

Example 7.3. *Consider the poset $(2^{[n]}, \subseteq)$, where "$\subseteq$" denotes the inclusion relationship.*

We often use "$\preccurlyeq$" to replace the use of "R". So poset $(X, R) = (X, \preccurlyeq)$ and $xRy = x \preccurlyeq y$. If $x \preccurlyeq y$ but $x \ne y$, then $x \prec y$, and we say x is a predecessor/child of y.

Definition 7.4. *Let $(X, \preccurlyeq)$ be a poset. We say an element x is an immediate predecessor of y, if*

(1) $x \prec y$,

(2) there is no element $t \in X$ such that $x \prec t \prec y$.

In this case, we write $x \lhd y$.

Fact 7.5. *For $x, y \in (X, \preccurlyeq)$, $x \prec y$ if and only if there exist $z_1, z_2, ..., z_k \in X$ such that $x \lhd z_1 \lhd z_2 \lhd ... \lhd z_k \lhd y$. (Note that here k can be 0, i.e., $x \lhd y$.)*

Proof. ($\Leftarrow$) This direction is trivial, by transitive property.

($\Rightarrow$) Let $x \prec y$. Let $M_{xy} = \{t \in X : x \prec t \prec y\}$. We prove by induction on $|M_{xy}|$.

Base case is clear, if $|M_{xy}| = 0$, then $x \lhd y$. Now we may assume $M_{xy} \neq \emptyset$ and the statement holds for any $u \prec v$ with $|M_{uv}| < n$. Suppose $x \prec y$ with $|M_{xy}| = n \geqslant 1$. Pick any $t \in M_{xy}$ and consider M_{xt} and M_{ty}. Clearly $M_{xt} \subsetneq M_{xy}$ and $M_{ty} \subsetneq M_{xy}$ (because of transitive property). By induction on M_{xt} and M_{ty}, there exist $x_1, x_2, ..., x_m \in X$ and $y_1, y_2, ..., y_l \in X$ such that $x \lhd x_1 \lhd x_2 \lhd ... \lhd x_m \lhd t$ and $t \lhd y_1 \lhd y_2 \lhd ... \lhd y_l \lhd y$. Thus, $x \lhd x_1 \lhd x_2 \lhd x_m \lhd t \lhd y_1 \lhd ... \lhd y_l \lhd y$ and we are done. ∎

Now we can express a poset in a diagram.

Definition 7.6. *The Hassa diagram of a poset $(X, \preccurlyeq)$ is a drawing in the plane such that*

(1) each element of X is drawn as a nod in the plane,

(2) each pair $x \lhd y$ is connected by a line segment,

(3) if $x \lhd y$, then the nod x must appear lower in the plane then the nod y.

The fact that $x \prec y$ if and only if $x \lhd x_1 \lhd x_2 \lhd ... \lhd x_k \lhd y$ now can be restated as follows: $x \prec y$ if and only if we can find a path in the Hassa diagram from nod x to nod y, strictly from bottom to top.

Definition 7.7. *Let $(X_1, \preccurlyeq_1)$ and $(X_2, \preccurlyeq_2)$ be two posets. A mapping $f : X_1 \to X_2$ is called an embedding of $(X_1, \preccurlyeq_1)$ in $(X_2, \preccurlyeq_2)$ if*

(1) f is injective,

(2) $f(x) \preccurlyeq_2 f(y)$ if and only if $x \preccurlyeq_1 y$.

Theorem 7.8. *For every poset $(X, \preccurlyeq)$ there exists an embedding of $(X, \preccurlyeq)$ in $\mathscr{B}_X = (2^X, \subseteq)$.*

Proof. Consider the mapping $f : X \to 2^X$ by letting $f(x) = \{y \in X : \ y \preccurlyeq x\}$ for any $x \in X$. It suffices to verify that f is an embedding of $(X, \preccurlyeq)$ in $(2^X, \subseteq)$.

Firstly, f is injective. If $f(x) = f(y)$ for $x, y \in X$, then $x \in f(x) = f(y)$ and $x \preccurlyeq y$. Similarly we have $y \preccurlyeq x$. So $x = y$.

Secondly, $f(x) \subseteq f(y)$ if and only if $x \preccurlyeq y$. To see this, if $x \preccurlyeq y$, then clearly $f(x) \subseteq f(y)$. Now suppose $f(x) \subseteq f(y)$. Since $x \in f(x) \subseteq f(y)$, we have $x \preccurlyeq y$. This shows that f indeed is an embedding. ∎

Definition 7.9. *Let $P = (X, \preccurlyeq)$ be a poset.*

(1) For distinct $x, y \in X$, if $x \prec y$ or $y \prec x$, then we say that x, y are comparable; otherwise, x, y are incomparable.

(2) The set $A \subseteq X$ is an antichain of P, if any two elements in A are incomparable. Let $\alpha(P)$ be the maximum size of an antichain of P.

(3) The set $B \subseteq X$ is a chain of P, if any two elements of B are comparable. Let $\omega(P)$ be the maximum size of a chain of P.

Consider the Hassa diagram, $\omega(P)$ means the maximum number of vertices in a path (from bottom to top) in this diagram. So $\omega(P)$ is also called the height of P and $\alpha(P)$ is called the width of P.

Definition 7.10. *An element $x \in X$ is minimal in $P = (X, \preccurlyeq)$, if x has no predecessor in P.*

Fact 7.11. *The set of all minimal elements of $P = (X, \preccurlyeq)$ forms an antichain of P.*

Theorem 7.12. *For any poset $P = (X, \preccurlyeq)$, $\alpha(P) \cdot \omega(P) \geq |X|$.*

Proof. We inductively define a sequence of posets $P_i = (X_i, \preceq)$ and a sequence of sets $M_i \subset P_i$, such that each M_i is the set of minimal elements of P_i, and $X_i = X - \sum_{j=0}^{i-1} M_j$, where $M_0 = \emptyset$.

First, set $P_1 = P = (X, \preccurlyeq), X_1 = X$ and $M_1 = \emptyset$. Assume posets $P_i = (X_i, \preccurlyeq)$ and M_{i-1} are defined for all $1 \leqslant i \leqslant k$. Let $M_i = \{$ all minimal elements of $P_i\}$ and let $X_{i+1} = X - M_1 \bigcup ... \bigcup M_i$. Then let P_{i+1} be the subposet of P restricted on X_{i+1}. We keep doing this until $X_{\ell+1} = \emptyset$. By Fact 7.11, each M_i is an antichain of P_i. Since P_i is the restricted subposet of P on X_i, M_i is also an antichain of P. So

$$|M_i| \leq \alpha(P).$$

It suffices to find a chain $x_1 \prec x_2 \prec ... \prec x_\ell$ in P, such that $x_i \in P_i = (X_i, \preccurlyeq)$ for $i \in [\ell]$. Indeed, if this holds, then

$$X = M_1 \bigcup M_2 \bigcup ... \bigcup M_\ell \text{ and } |X| = \sum_{i=1}^{\ell} |M_i| \leq \alpha(P) \cdot \ell \leq \alpha(P) \cdot \omega(P).$$

In fact, by the definition of M_i, we can claim something stronger holds: For any $x \in M_i$ ($2 \leq i < \ell$), there exists $y \in M_i$, such that $y \prec x$. This completes the proof. ∎

7.2 The Order From Disorder

Definition 7.13. *Consider a sequence $X = (x_1, x_2, ..., x_n)$ of n real numbers. A subsequence $(x_{i_1}, x_{i_2}, ..., x_{i_m})$ of X, where $i_1 < i_2 < ... < i_m$, is* monotone*, if either $x_{i_1} \leq x_{i_2} \leq ... \leq x_{i_m}$ or $x_{i_1} \geq x_{i_2} \geq ... \geq x_{i_m}$.*

For example, $(10, 9, 7, 4, 5, 1, 2, 3) \longrightarrow (10, 9, 7, 5, 1)$.

Theorem 7.14 (Erdős-Szekeres Theorem)**.** *For any sequence $(x_1, x_2, ..., x_{n^2+1})$ of length $n^2 + 1$, there exists a monotone subsequence of length $n + 1$.*

Proof. Let $X = [n^2 + 1]$. We define a poset $P = (X, \preceq)$ as following: $i \preceq j$ if and only if $i \leq j$ and $x_i \leq x_j$.

It is easy to check that $P = (X, \preceq)$ indeed defines a poset (reflective antisymmetric and transitive). By the previous result that $\alpha(P) \cdot w(P) \geq |X| = n^2 + 1$, we have either $w(P) \geq n + 1$ or $\alpha(P) \geq n + 1$.

Case 1. $w(P) \geq n + 1$.

There exists a chain of size $n + 1$, say $\{i_1, i_2, .., i_{n+1}\}$. By definition, $x_{i_1} \leq x_{i_2} \leq ... \leq x_{i_{n+1}}$ is an increasing subsequence of length $n + 1$.

Case 2. $\alpha(P) \geq n + 1$.

There exists an antichain of size n+1, say $\{i_1, i_2, .., i_{n+1}\}$. We may assume that $i_1 < i_2 < ... < i_{n+1}$ being antichain, it implies that $x_{i_1} > x_{i_2} > ... > x_{i_{n+1}}$ is a decreasing subsequence of $(x_1, x_2, ..., x_{n^2+1})$.

∎

Remark 7.15. *What we proved is a bit stronger: there is either an increasing subsequence of length $n+1$ or a strictly decreasing subsequence of length $n+1$.*

Exercise 7.16. *Find examples to show that Erdős-Szekeres Theorem is optimal: there exists a sequence of n^2 reals such that NO monotone subsequence of length $n+1$.*

7.3 The Pigeonhole Principle

Theorem 7.17 (The Pigeonhole Principle)**.** *Let X be a set with at least $1+\sum_{i=1}^{k}(n_i-1)$ elements and let $X_1, X_2, ..., X_k$ be disjoint sets forming a partition of X. Then, there exists some i, such that $|X_i| \geq n_i$.*

(1) Two equal degrees.

Theorem 7.18. *Any graph has two vertices of the same degree.*

Proof. Let G be a graph with n vertices. Suppose that G does not have two vertices of same degree. So the only exceptional case will be that there is exactly one vertex of degree i for all $i \in \{0, 1, ..., n-1\}$. But this is impossible to have a vertex with degree 0 and a vertex with degree $n-1$ at the same time. ∎

Exercise 7.19. *For any n, find an n-vertex graph G, which has exactly two vertices with the same degree.*

(2) Subsets without divisors.

Question 7.20. *How large a subset $S \subset [2n]$ can be such that for any $i, j \in S$, we have $i \nmid j$ and $j \nmid i$?*

Obviously, we can take $S = \{n+1, n+2, ..., 2n\}$ with $|S| = n$.

Theorem 7.21. *For any $S \subset [2n]$ with $|S| \geq n+1$, there exist $i, j \in S$ such that $i|j$.*

Proof. For any odd integer $2k-1 \in [2n]$, define $S_{2k-1} = \{2^i \cdot (2k-1) \in S : i \geq 0\}$. Clearly, $S = \bigcup_{k=1}^{n} S_{2k-1}$. Since $|S| \geq n+1$, there exists some $|S_{2k-1}| \geq 2$ say $x, y \in S_{2k-1}$. It is easy to see that we have $x|y$ or $y|x$. ∎

(3) Rational approximation.

Theorem 7.22. *Given $n \in \mathbb{Z}^+$, for any $x \in \mathbb{R}^+$, there is a rational number $\frac{p}{q}$ such that $1 \leq q \leq n$ and $|x - \frac{p}{q}| < \frac{1}{nq}$.*

Proof. For any $x \in \mathbb{R}^+$, define $\{x\} = x - \lfloor x \rfloor$ be the fractional part of x. Consider $\{ix\} \in [0,1)$, for any $i = 1, 2, ..., n+1$. Partition $[0,1)$ into n subintervals $[0, \frac{1}{n}), [\frac{1}{n}, \frac{2}{n}), ..., [\frac{n-1}{n}, 1)$. By Pigeonhole Principle, there exists a subinterval $[\frac{k}{n}, \frac{k+1}{n})$ contains two reals say $\{ix\}$ and $\{jx\}$ for $1 \leq i < j \leq n+1$. Then we have $\{(j-i)x\} \in [0, \frac{1}{n}) \cup [1-\frac{1}{n}, 1)$. Let $q = j - i \leq n$. So $\{qx\} \in (0, \frac{1}{n}) \cup [1-\frac{1}{n}, 1)$, i.e. $qx = p + \epsilon$ for some $p \in \mathbb{Z}^+$ and $|\epsilon| < \frac{1}{n}$. Then we have $x = \frac{p}{q} + \frac{\epsilon}{q}$, which implies that $|x - \frac{p}{q}| = |\frac{\epsilon}{q}| < \frac{1}{nq}$. ∎

7.4 Second Proof of Erdős-Szekeres Theorem

Theorem 7.23 (Erdős-Szekeres Theorem)**.** *For any sequence of* $mn+1$ *real numbers* $\{a_0, a_1, ..., a_{mn}\}$*, there is an increasing subsequence of length* $m+1$ *or a decreasing subsequence of length* $n+1$*.*

The second proof. Consider any sequence $\{a_0, a_1, ..., a_{mn}\}$. For any $i \in \{0, 1, ..., mn\}$, let f_i be the maximum size of an increasing subsequence starting at a_i. We may assume $f_i \in \{1, 2, ..., m\}$ for any $i \in \{0, 1, ..., mn\}$. By Pigeonhole Principle, there exists a $s \in \{1, 2, ..., m\}$ such that there are at least $n+1$ elements $i \in \{0, 1, ..., m\}$ satisfying $f_i = s$. Let these elements be $i_1 < i_2 < ... < i_{n+1}$.

We claim that $a_{i_1} \geq a_{i_2} \geq ... \geq a_{i_{n+1}}$. Indeed, If $a_{i_j} < a_{i_{j+1}}$ for some $j \in [n]$, then we would extend the maximum increasing subsequence of length s starting at $a_{i_{j+1}}$ by adding a_{i_j} to obtain an increasing subsequence starting at a_{i_j} of length s+1, a contradiction to $f_{i_j} = s$.

∎

8 Ramsey's Theorem

Fact 8.1 (A party of six)**.** *Suppose a party has six participants. Participants may know each other or not. Then there must be three participants who know each other or do not know each other, i.e. any* 6*-vertex graph* G *has a* K_3 *or* I_3*.*

Proof. We consider a graph G on six vertices say $[6]$. Each vertex i represents one participant: i and j are adjacent if and only if they know each other. Then we need to show that there are three vertices in G which form a triangle K_3 or an independent set I_3.

Consider vertex 1. There are five other persons. So 1 is adjacent to three vertices or not adjacent to three vertices. By symmetry, we may assume that 1 is adjacent to three vertices, say $2, 3, 4$. If one of pairs $\{2, 3\}, \{2, 4\}, \{3, 4\}$ is adjacent, then we have a K_3. Otherwise, $\{2, 3, 4\}$ forms an independent set of size three. This finishes the proof. ∎

Definition 8.2. *An* r*-edge-coloring of* K_n *is a mapping* $f : E(K_n) \longrightarrow \{1, 2, ..., r\}$ *which assigns one of the colors* $1, 2, ..., r$ *to each edge of* K_n*.*

Definition 8.3. *Given an* r*-edge-coloring of* K_n*. A clique in* K_n *is called* monochromatic*, if all its edges are colored by the same color.*

Then the example of a party of six says that any 2-edge-coloring of K_6 has a monochromatic K_3.

Theorem 8.4 (Ramsey's Theorem (2-colors-version))**.** *Let* $k, \ell \geq 2$ *be any two integers. Then there exists an integer* $N = N(k, \ell)$*, such that any* 2*-edge-coloring of* K_N *(with colors red and blue) has a blue* K_k *or a red* K_ℓ*.*

Proof. We will prove by induction on $k+\ell$ that any blue/red-edge-coloring of a clique on $N = \binom{k+\ell-2}{k-1}$ vertices has a blue K_k or a red K_ℓ.

Base case is trivial (as we have $N = \binom{k+\ell-2}{k-1} = \ell$ where $k = 2$ and $N = \binom{k+\ell-2}{k-1} = k$ where $\ell = 2$).

We may assume that the statement holds for $k'+\ell' \leq k+\ell-1$. Let $N_1 = \binom{k+\ell-3}{k-2}$, $N_2 = \binom{k+\ell-3}{k-1}$, and $N = \binom{k+\ell-2}{k-1}$. So $N_1 + N_2 = N$.

Consider any red/blue-edge-coloring of K_N. Consider any vertex x. Let $A = \{y \in V(K_n) - \{x\} : \text{edge } xy \text{ is blue}\}$ and $B = \{y \in V(K_n) - \{x\} : \text{edge } xy \text{ is red}\}$. So $|A| + |B| = N - 1 = N_1 + N_2 - 1$. By Pigeonhole Principle we have either $|A| \geq N_1$ or $|B| \geq N_2$.

Case 1. $|A| \geq N_1 = \binom{(k-1)+\ell-2}{(k-1)-1}$.

The vertices of A contains a $K_{\binom{(k-1)+\ell-2}{(k-1)-1}}$ where edges are blue or red. By induction on this $K_{\binom{(k-1)+\ell-2}{(k-1)-1}}$ for the pair $\{k-1, \ell\}$, so A has a blue K_{k-1} or a red K_ℓ. In the former, by adding the vertex x to that blue K_{k-1}, we can obtain a blue K_k in the K_N.

Case 2.$|B| \geq N_2 = \binom{k+\ell-3}{k-1}$.

This case is similar (by induction on $\{k, \ell-1\}$). ∎

Definition 8.5. *For $k, \ell \geq 2$, the* Ramsey Number $R(k, \ell)$ *denotes the smallest integer N such that any 2-edge-coloring of K_N has a blue K_k or a red K_ℓ.*

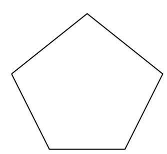
Remark 8.6. *Ramsay Theorem says that $R(k, \ell) \leq \binom{k+\ell-2}{k-1}$.*

Let us try to understand this definition a bit more:

- $R(k, \ell) \leq L$ if and only if any 2-edge-coloring of K_L has a blue K_k or a red K_ℓ.
- $R(k, \ell) > M$ if and only if there exists a 2-edge-coloring of K_M which has no blue K_k nor red K_ℓ.

Fact 8.7. *(1) $R(k, \ell) = R(\ell, k)$.*
(2) $R(2, \ell) = \ell$ and $R(k, 2) = k$.
(3) $R(3, 3) = 6$.

Proof. It is easy to know that (1) and (2) is right. We have $R(3, 3) \leq 6$ from the fact on a party of six. On the other hand, we have $R(3, 3) > 5$ from the following graph (if u, v are adjacent, we color edge uv blue, otherwise we color edge uv red).



∎

Exercise 8.8. $R(k, \ell) \leq R(k-1, \ell) + R(k, \ell-1)$.

Theorem 8.9. *If for some (k, ℓ), the numbers $R(k-1, \ell)$ and $R(k, \ell-1)$ are even, then*

$$R(k, \ell) \leq R(k-1, \ell) + R(k, \ell-1) - 1.$$

Proof. Let $n = R(k-1, \ell) + R(k, \ell-1) - 1$. So n is odd. Consider any 2-edge-coloring of K_n. For any vertex x, define the following as before $A_x = \{y : xy \text{ is blue}\}$ and $B_x = \{y : xy \text{ is red}\}$.

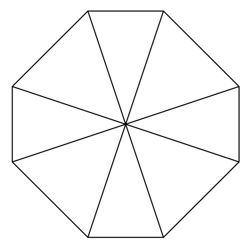
The previous proof tells us that if $|A_x| \geq R(k-1, \ell)$ or $|B_x| \geq R(k, \ell-1)$, then we can find a blue K_k or a red K_ℓ. Thus, we may assume that $|A_x| \leq R(k-1, \ell) - 1$ and $|B_x| \leq R(k, \ell-1) - 1$ for any vertex v, which implies that

$$n \leq A_x + B_x + 1 \leq R(k-1, \ell) + R(k, \ell-1) - 1$$

This shows that for each x, $|A_x| = R(k-1,\ell)-1$ and $|B_x| = R(k,\ell-1)-1$. Now we consider the graph G consisting of all blue edges. Note that G has an odd number of vertices and any vertex has odd degree. But this contradicts the Handshaking Lemma. ∎

Corollary 8.10. $R(3,4) = 9$.

Proof. By the previous theorem, we have $R(3,4) \le R(2,4)+R(3,3)-1 = 4+6-1 = 9$. On the other hand, we have $R(3,4) > 8$ from the following graph (if u, v are adjacent, we color edge uv blue, otherwise we color edge uv red).



∎

Definition 8.11. *For any $k \ge 2$ and any integers $s_1, s_2, ..., s_k \ge 2$, the Ramsey number $R_k(s_1, s_2, ..., s_k)$ is the least integer N such that any k-edge-coloring of K_N has a clique K_{s_i} in color i, for some $i \in [k]$.*

Homework 8.12. $R_k(s_1, s_2, ..., s_k) < +\infty$.

Theorem 8.13 (Schur's Theorem)**.** *For $k \ge 2$, there exists some integer $N = N(k)$ such that for any coloring $\varphi : [N] \to [k]$, there exist three integers $x, y, z \in [N]$ satisfying that $\varphi(x) = \varphi(y) = \varphi(z)$ and $x + y = z$.*

Proof. Let $N = R_k(3, 3, ..., 3)$. Define a k-edge-coloring of K_N from the coloring φ as following: for any $i, j \in [N]$, define the color of ij to be $\varphi(|i-j|)$. By the definition of $R_k(3, 3, ..., 3)$, we can find a monochromatic triangle, say $ij\ell$. Suppose $i < j < \ell$, we have $\varphi(\ell-j) = \varphi(\ell-i) = \varphi(j-i)$. Let $x = \ell-j, y = \ell-i, z = j-i \in [N]$, we have $\varphi(x) = \varphi(y) = \varphi(z)$ and $x+y = z$. This finishes the proof. ∎

Remark 8.14. *It is also true to require x, y, z to be distinct, by considering $N = R_k(4, 4, ..., 4)$.*

Using this theorem, Schur proved that the restricted version of Fermat's last problem in $\mathbb{Z}_p$ for sufficiently large prime p.

Theorem 8.15 (Schur)**.** *For any integer $m \ge 1$, there is an integer $p(m)$ such that for any prime $p \ge p(m)$, $x^m + y^m = z^m \pmod p$ has a nontrivial solution in $\mathbb{Z}_p$.*

Proof. For prime p, consider the multiplicative group $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$. Let g be a generator of $\mathbb{Z}_p^*$. Then for $x \in \mathbb{Z}_p^*$, there exists exactly one pair of integers (i, j) such that $x = g^{im+j} \pmod p$ for some $0 \le j \le m-1$ and $0 \le im+j \le p-2$. Then we define a coloring $\varphi : \mathbb{Z}_p^* \to \{0, 1, ..., m-1\}$ by letting $\varphi(x) = j$.

By Schur's Theorem, choose $p(m) = N(m)$, and for any $p \geq p(m)$, the coloring φ gives $x, y, z \in \mathbb{Z}_p^*$ satisfying $\varphi(x) = \varphi(y) = \varphi(z)$ and $x+y=z$. Let $x = g^{i_1 m+j},\ y = g^{i_2 m+j},\ z = g^{i_3 m+j} \pmod{p}$. Then $x+y=z$ implies that

$$g^{i_1 m+j} + g^{i_2 m+j} = g^{i_3 m+j} \pmod{p}, \tag{8.8}$$

thus

$$g^{i_1 m} + g^{i_2 m} = g^{i_3 m} \pmod{p}.$$

Let $\alpha = g^{i_1},\ \beta = g^{i_2},\ \gamma = g^{i_3}$. We have

$$\alpha^m + \beta^m = \gamma^m \pmod{p}.$$

∎

Remark: Schur's theorem holds in $\mathbb{Z}$, but we need to restrict the calculation in a multiplication cyclic group when deducing equation (8.8).

Definition 8.16. *A probability space is a pair (Ω, P), where Ω is a finite set and $P : 2^\Omega \to [0,1]$ is a function assigning a number in the interval $[0,1]$ to every subset of Ω such that*

(i) $P(\emptyset) = 0$,

(ii) $P(\Omega) = 1$, *and*

(iii) $P(A \cup B) = P(A) + P(B)$ *for disjoint sets* $A, B \subset \Omega$.

We say

- Any subset A of Ω is called an event, and $P(A) = \sum_{\omega \in \Omega} P(\{\omega\})$.
- A random variable is a function $X : \Omega \to R$
- The expectation of a random variable X is:

$$E[X] := \sum_{\omega \in \Omega} P(\{\omega\}) \cdot X(\omega).$$

The linearity of expectations: for any two random variables X and Y on Ω, we have

$$E[X+Y] = E[X] + E[Y].$$

Now we discuss the following basic form of the probabilistic methods in Combinatorics:

(i) Imagine we need to find some combinatorial object satisfying certain property, call it a "good" property. We consider a big family for candidates and randomly pick one from this family, call it a random object. If the probability that the random object has "good" property is positive, then there must exist "good" objects.

(ii) To compute the probability of being "good", we often compute the probability of being "bad" and aim to show that this probability of being "bad" is strictly less than 1.

Theorem 8.17. *Let n, s satisfy $\binom{n}{s} \cdot 2^{1-\binom{s}{2}} < 1$. Then $R(s,s) > n$.*

Proof. We need to find a 2-edge-coloring of K_n such that it has no monochromatic clique K_s.

Let Φ be the family of all 2-edge-colorings of K_n. Let $c \in \Phi$ be chosen uniformly at random. Then c is a random 2-edge-coloring of K_n, where each edge of K_n is colored by red and blue, each with probability $\frac{1}{2}$, independent of each other edge.

Let B be the event that this random 2-edge-coloring has no monochromatic K_s. We want to prove $P(B) > 0$. Consider its complement event $A = \Omega \backslash B$ and its probability $P(A)$, where A is the event that c has a monochromatic K_s. For any $S \in \binom{[n]}{s}$, let A_S be the event that S forms a monochromatic K_s for c. So $A = \cup_{S \in \binom{[n]}{s}} A_S$, and $P(A_S) = 2^{1-\binom{s}{2}}$.

Thus

$$P(A) = P\left(\cup_{S \in \binom{[n]}{s}} A_S\right) \leq \sum_{S \in \binom{[n]}{s}} P(A_S) = \binom{n}{s} 2^{1-\binom{s}{2}} < 1,$$

This shows that $P(B) > 0$. ∎

Corollary 8.18. $R(s,s) \geq \frac{1}{e\sqrt{2}} s 2^{\frac{s}{2}}$.

Proof. Let $n = \frac{1}{e\sqrt{2}} s 2^{\frac{s}{2}} \left(\frac{e}{2}\right)^{1/s}$. Recall that $\binom{n}{s} < \frac{n^s}{s!}$ and $s! \geq e\left(\frac{s}{e}\right)^s$, thus we have that

$$\binom{n}{s} 2^{1-\binom{s}{2}} < \frac{n^s}{e\left(\frac{s}{e}\right)^s} 2^{1-\binom{s}{2}} = 1.$$

So by the above theorem, we get

$$R(s,s) > n = \frac{1}{e\sqrt{2}} s 2^{\frac{s}{2}} \left(\frac{e}{2}\right)^{1/s} \geq \frac{1}{e\sqrt{2}} s 2^{\frac{s}{2}}.$$

∎

Definition 8.19. *The random graph $G(n,p)$ for some real $p \in (0,1)$ is a graph with vertex set $\{1, 2, ..., n\}$, where each of potential $\binom{n}{2}$ edges appears with probability p, independent of other edges.*

In the proof of the previous theorem, in fact we consider $G(n, 1/2)$.

Let A be the property we are interested in. Let

$$\begin{aligned} P(A) &= P(G(n, \frac{1}{2}) \text{ satisfies the property } A) \\ &= \frac{\text{the number of graphs with vertex set } [n] \text{ satisfying the property } A}{2^{\binom{n}{2}}}. \end{aligned}$$

So $P(A)$ is a function of n, taking value in $[0,1]$.

Definition 8.20. *We say the random graph $G(n, \frac{1}{2})$ almost surely satisfies property A, if*

$$\lim_{n \to +\infty} P_r(A) = 1.$$

If $\lim_{n \to +\infty} P_r(A) = 0$, then $G(n, \frac{1}{2})$ almost surely does not satisfy the property A.

Theorem 8.21. *Random graph $G(n, \frac{1}{2})$ almost surely is not bipartite.*

Proof. Let A be the event that $G(n, \frac{1}{2})$ is bipartite. For any $U \subseteq [n]$, let A_U be the event that all edges of G are between U and $[n]\backslash U$. Then $A = \bigcup_{U \subseteq [n]} A_U$. We have

$$P(A_U) = \frac{\text{the number of graphs satisfying } A_U}{2^{\binom{n}{2}}} = \frac{2^{|U|(n-|U|)}}{2^{\binom{n}{2}}} \leq \frac{2^{\frac{n^2}{4}}}{2^{\frac{n(n-1)}{2}}} = 2^{-\frac{n^2}{4}+\frac{n}{2}}.$$

So by the union bound,

$$0 \leq P(A) = P(\bigcup_{U \subseteq [n]} A_U) \leq \sum_{U \subseteq [n]} P(A_U) \leq 2^n \cdot 2^{-\frac{n^2}{4}+\frac{n}{2}} = 2^{-\frac{n^2}{4}+\frac{3n}{2}}.$$

Thus $\lim_{n \to +\infty} P(A) = 0$. ∎

9 The Probabilistic Method

Definition 9.1. *Let $\mathcal{F}$ be a family of subsets of set Ω. We say $\mathcal{F}$ is a k-family if all its subsets have size k.*

Example 9.2. *A 2-family is just a graph.*

Definition 9.3. *We say $\mathcal{F}$ is 2-colorable if there exists a function $f : \Omega \to \{blue, red\}$ such that every subset A in $\mathcal{F}$ is not monochromatic (i.e., each A contains at least one blue vertex and at least one red vertex.)*

Definition 9.4. *For any $k \in Z^+$, let $m(k)$ be the minimum number of subsets in a k-family $\mathcal{F}$ which is not 2-colorable.*

Therefore, we see that $m(k) \leq t$ if and only if there exists a k-family $\mathcal{F}$ of t subsets which is not 2-colorable, and $m(k) > t$ if and only if any k-family of t subsets can be 2-colorable.

Fact 9.5. $m(2) = 3$. *Consider the graph K_3.*

Theorem 9.6. *For any k, we have $m(k) > 2^{k-1} - 1$, i.e., any k-family $\mathcal{F}$ of $2^{k-1} - 1$ subsets can be 2-colorable.*

Proof. Given a k-family $\mathcal{F}$ of $2^{k-1} - 1$ subsets, we aim to find a function $f : \Omega \to \{\text{blue,red}\}$ such that any subset A in $\mathcal{F}$ has a blue vertex and a red vertex. We call such f "good".

Now we consider a random function $\varphi : \Omega \to \{\text{blue,red}\}$, that is, each $x \in \Omega$ is colored by blue or red with probability $\frac{1}{2}$, independent of other choices.

Let S be the event that the random function φ is good. Let $T = S^c$ be the complement, i.e., there exists a subset A in $\mathcal{F}$ which is monochromatic under φ. For each $A \in \mathcal{F}$, let T_A be the event that the subset A is monochromatic under φ. So

$$T = \bigcup_{A \in \mathcal{F}} T_A.$$

It is easy to see that

$$P(T_A) = 2(\frac{1}{2})^k = 2^{1-k}.$$

So by the union bound,

$$P(T) = P(\bigcup_{A\in\mathcal{F}} T_A) \le \sum_{A\in\mathcal{F}} P(T_A) = |\mathcal{F}|2^{1-k} < 1.$$

Therefore, we have

$$P(\varphi \text{ is good}) = P(S) = 1 - P(T) > 0.$$

Since

$$P(\varphi \text{ is good}) = \frac{\text{number of good functions}}{\text{total number of functions}}.$$

We know that there exists at least one good function $f : \Omega \to \{\text{blue,red}\}$. ∎

Definition 9.7. *Given a probability space (Ω, P), we say events $A_1, A_2, ..., A_k$ are* independent *if for any $I \subset [n]$, we have $P(\bigcap_{i\in I} A_i) = \prod_{i\in I} P(A_i)$.*

Definition 9.8. *A* tournament *on n vertices is a directed graph obtained from the clique K_n by assigning a direction to each edge of K_n. For any arc $i \to j$, we say i is the head and j is the tail of the arc.*

Definition 9.9. *A tournament T satisfies the property S_k if for any subset A of size k, there exists a vertex $u \in V(T) \setminus A$ such that $u \to x$ for any $x \in A$.*

Question 9.10. *For any $k \in Z^+$, can we find a tournament satisfying the property S_k?*

Theorem 9.11. *For any $k \in Z^+$, if $\binom{n}{k}(1 - \frac{1}{2^k})^{n-k} < 1$, then there exists a tournament on n vertices satisfying the property S_k.*

Proof. We prove this by considering a random tournament T on $[n]$, that is, for any pair $\{i, j\}$, the arc $i \to j$ occurs with probability $\frac{1}{2}$, independent of other choices. Let B be the event that T does not satisfy the property S_k. For $A \in \binom{[n]}{k}$, let B_A be the event that for every vertex $x \in [n] \setminus A$ there exists some $u \in A$ with $u \to x$. So

$$B = \bigcup_{A\in\binom{[n]}{k}} B_A.$$

For $x \in [n]\setminus A$, let $B_{A,x}$ be the event that there exists some $u \in A$ with $u \to x$. So

$$B_A = \bigcap_{x\in[n]\setminus A} B_{A,x}.$$

It is easy to see that for any $x \in [n] \setminus A$

$$P(B_{A,x}) = 1 - \left(\frac{1}{2}\right)^k.$$

Note that only the arcs between x and A will effect the event $B_{A,x}$, and these arcs for distinct vertices x's are disjoint. This explains that all events $B_{A,x}$ for all $x \in [n] \setminus A$ are independent. So

$$P(B_A) = P(\bigcap_{x\notin A} B_{A,x}) = \prod_{x\notin A} P(B_{A,x}) = \left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k}.$$

Therefore,

$$P(B) \le \sum_{A \in \binom{[n]}{k}} P(B_A) \le \binom{n}{k} \left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} < 1.$$

Thus, $P(B^c) > 0$, i.e., there exists a tournament on $[n]$ satisfying property S_k.

∎

Corollary 9.12. *For any $k \in Z^+$, there exists a minimal $f(k)$ such that there exists a tournament on $f(k)$ vertices satisfying the property S_k.*

Example 9.13. *We have $f(3) \le 91$, as $\binom{91}{3}(\frac{7}{8})^{88} < 1$.*

9.1 The Linearity of Expectation

- For any two variables X, Y, we have $E[X+Y] = E[X] + E[Y]$.
- $P(X \ge E[X]) > 0$.
- $P(X \le E[X]) > 0$.

Definition 9.14. *A set A is sum-free, if for any $x, y \in A, x + y \notin A$, i.e., $x + y = z$ has no solutions in A.*

Example: Both $\{\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 2, ..., n\}$ and $\{$all odd integers in $[n]\}$ are two sum-free sets in $[n]$ of size $\lceil \frac{n}{2} \rceil$.

Exercise 9.15. *Show that the maximum size of a sum-free subset A in $[n]$ is $\lceil \frac{n}{2} \rceil$.*

Theorem 9.16. *For any set A of non-zero integers, there exists a sum-free subset $B \subseteq A$ with $|B| \ge \frac{|A|}{3}$.*

Proof. We choose a prime p large enough such that $p > |a|$ for any $a \in A$. Consider $Z_p = \{0, 1, ..., p-1\}$ and $Z_p^* = \{1, 2, ..., p-1\}$. We note that there is a large sum-free subset under Z_p(mod p):

$$S = \left\{ \lceil \frac{p}{3} \rceil + 1, \lceil \frac{p}{3} \rceil + 2, ..., \lceil \frac{2p}{3} \rceil \right\}.$$

Claim: For any $x \in Z_p^*$, $A_x = \{a \in A : ax \pmod{p} \in S\}$ is sum-free.

Proof. Suppose that there are $a, b, c \in A_x$ satisfying $a + b = c$. But we also have $ax \pmod{p} \in S$, $bx \pmod{p} \in S$, $cx \pmod{p} \in S$ and $ax \pmod{p} + bx \pmod{p} = cx \pmod{p}$ in Z_p. This is a contradiction to that S is sum-free in Z_p. ∎

Next, we want to find some $x \in Z_p^*$ such that $|A_x| \ge \frac{|A|}{3}$. We choose $x \in Z_p^*$ uniformly at random, and we compute, $E\big[|A_x|\big]$, the expectation of $|A_x|$.

Note that $|A_x| = \sum\limits_{a \in A} 1_{\{ax \pmod{p} \in S\}}$. So

$$E\big[|A_x|\big] = E\Big[\sum_{a \in A} 1_{\{ax \pmod{p} \in S\}}\Big] = \sum_{a \in A} E\big[1_{\{ax \pmod{p} \in S\}}\big] = \sum_{a \in A} P\big(ax \pmod{p} \in S\big).$$

We observe that for a fixed $a \in A$, $\{ax : x \in Z_p^*\} = Z_p^*$. So $P\big(ax \pmod p \in S\big) = \frac{|S|}{|Z_p^*|} \geq \frac{1}{3}$. And thus, $E\big[|A_x|\big] \geq \sum_{a \in A} \frac{1}{3} = \frac{|A|}{3}$. Then, we know that there exists a choice of $x \in Z_p^*$ such that $|A_x| \geq E\big[|A_x|\big] \geq \frac{|A|}{3}$. ∎

Definition 9.17. *Given a graph G, a dominating set A in G is a subset of $V(G)$ such that any $u \in V(G) \backslash A$ has a neighbor in A.*

Theorem 9.18. *Let G be a graph on n vertices and with minimum degree $\delta > 1$. Then G contains a dominating set of at most $\dfrac{1+\ln(1+\delta)}{1+\delta}n$ vertices.*

Proof. Take $p \in (0,1)$, whose value will be determined later. We pick each vertex in $V(G)$ with probability p uniformly at random. Let A be the set of those chosen vertices. Let B be the set of vertices $b \in V(G) \setminus A$, which has no neighbors in A. Then we can see that

- $A \cup B$ is a dominating set in G.
- $b \in B$ if and only if $\big(\{b\} \cup N_G(b)\big) \cap A = \emptyset$.

That is, $b \in B$ if and only if b and all neighbors of b are not picked. So

$$P(b \in B) = (1-p)^{1+d_G(b)} \leq (1-p)^{1+\delta} \leq e^{-p(1+\delta)},$$

where the last inequality holds since $1 + x \leq e^x$. Then, we have

$$E\big[|B|\big] = E\Big[\sum_{b \in V(G)} 1_{\{b \in B\}}\Big] = \sum_{b \in V(G)} P(b \in B) \leq n \cdot e^{-p(1+\delta)}.$$

We also have $E\big[|A|\big] = np$. Thus,

$$E\big[|A \cup B|\big] \leq E\big[|A| + |B|\big] = E\big[|A|\big] + E\big[|B|\big] \leq n\big(p + e^{-p(1+\delta)}\big).$$

By calculus, we see that when $p = \dfrac{\ln(1+\delta)}{1+\delta}$, $p + e^{-p(1+\delta)}$ is minimized with value $\dfrac{1+\ln(1+\delta)}{1+\delta}$. So we pick $p = \dfrac{\ln(1+\delta)}{1+\delta}$ to get $E\big[|A \cup B|\big] \leq \dfrac{1+\ln(1+\delta)}{1+\delta}n$. Therefore there exists a choice of $A \cup B$ such that $|A \cup B| \leq E\big[|A \cup B|\big] \leq \dfrac{1+\ln(1+\delta)}{1+\delta}n$, where $A \cup B$ is a dominating set of G. ∎

Definition 9.19. *Let $\alpha(G)$ be the maximum size of an independent set in G.*

Theorem 9.20. *For any graph G, $\alpha(G) \geqslant \sum_{v \in V(G)} \dfrac{1}{d(v)+1}$ where $d(v)$ denotes the degree of v in G.*

Proof. Let $V(G) = [n]$. For $i \in [n]$, let N_i be the neighborhood of i in G. Let S_n be the family of all permutations $\pi : [n] \to [n]$.

Given a permutation $\pi \in S_n$, we say a vertex $i \in [n]$ is $\pi-$good, if $\pi(i) < \pi(j)$ for any $j \in N_i$. Let M_π be the set of all π-good vertices.
Claim: For any $\pi \in S_n$, M_π is an independent set in G.

Proof. Suppose that there are two vertices $i, j \in M_\pi$ with $ij \in E(G)$. Let $\pi(i) < \pi(j)$. Then j is not π-good, a contradiction. ∎

We pick an $\pi \in S_n$ uniformly at random, and compute $E\big[|M_\pi|\big]$. Since $|M_\pi| = \sum\limits_{i\in[n]} 1_{\{i \text{ is } \pi\text{-good}\}}$, we have $E\big[|M_\pi|\big] = \sum\limits_{i\in[n]} P(i \text{ is } \pi\text{-good}) = \sum\limits_{i\in[n]} \dfrac{1}{d(i)+1}$. Thus there exists a permutation $\pi \in S_n$ such that $|M_\pi| \geq \sum\limits_{i\in[n]} \dfrac{1}{d(i)+1}$. Then by the definition of $\alpha(G)$ and our claim, we can get that $\alpha(G) \geq \sum\limits_{v\in V(G)} \dfrac{1}{d(v)+1}$ which completes the proof. ∎

Corollary 9.21. *For any graph G with n vertices and m edges, we have $\alpha(G) \geq \frac{n^2}{2m+n}$.*

Proof. Exercise. ∎

Corollary 9.22. *For any graph G with n vertices and average degree d (i.e., $d = \frac{2m}{n}$), then $\alpha(G) \geq \frac{n}{1+d}$.*

Definition 9.23. *Turán graph $T_r(n)$ on r parts is an n-vertex graph G such that $V(G) = V_1 \cup V_2 \cup ... \cup V_r$ and $|V_1| \leq |V_2| \leq ... \leq |V_r| \leq |V_1| + 1$, where $ab \in E(G)$ if and only if $a \in V_i$ and $b \in V_j$ for some $i \neq j$.*

$T_r(n)$ is a balanced complete r-partite graph.

Theorem 9.24 (Turán's Theorem approximate form)**.** *If G is K_{r+1}-free, then $e(G) \leqslant \dfrac{r-1}{2r} n^2$.*

Theorem 9.25 (Turán's Theorem exact form)**.** *If an n-vertex graph G is K_{r+1}-free, then $e(G) \leqslant$ $\mathrm{ex}(T_r(n)) \approx \dfrac{r-1}{2r} n^2$.*

We give two proofs for the approximate version of Turán's Theorem.

First proof. Using Corollary 9.22 (Exercise). ∎

Second proof. We are given an n-vertex K_{r+1}-free graph G, where $V(G) = [n]$. Consider a function $p : [n] \to [0, 1]$ such that

$$\sum_{i\in[n]} p_i = 1. \tag{9.9}$$

We want to find the maximum of $f(p) = \sum_{ij\in E(G)} p_i p_j$ over all such functions $p : [n] \to [0, 1]$. Suppose p is the function obtaining the maximum $f(p)$, and subject to this, the number of vertices i with $p(i) \neq 0$ is minimized.

Claim. $\{i : p(i) > 0\}$ is a clique in G.

Proof. Suppose NOT, say $p(i), p(j) > 0$ and $ij \notin E(G)$. Let $S_i = \sum_{k\in N_G(i)} p_k$ and $S_j = \sum_{k\in N_G(j)} p_k$. Let $S_i \geqslant S_j$. Then we can assign a new function $p^* : [n] \to [0, 1]$ such that

$$p^*(i) = p(i) + p(j),\ p^*(j) = 0 \text{ and } p^*(k) = p(k) \text{ for } k \in [n] \setminus \{i, j\}.$$

Now we have

$$f(p^*) = f(p) - (p_i S_i + p_j S_j) + (p_i + p_j)S_i = f(p) + (S_i - S_j)p_j \geqslant f(p).$$

By the choice of p, we see $f(p^*) = f(p)$, but p^* has fewer vertices i with positive weight than p, a contradiction. This proves the claim. ∎

Let $S = \{1, 2, ..., s\} \subseteq V(G)$ be the set of vertices with positive weight. Then by the claim, we see $G[S] = K_s$, where $s \leq r$ as G is K_{r+1}-free. Then

$$\begin{aligned}\max_p f(p) =& \frac{1}{2}\left[(\sum_{1\leq i\leq s} p(i))^2 - \sum_{1\leq i\leq s} p^2(i)\right] = \frac{1}{2}[1 - \sum_{1\leq i\leq s} p^2(i)] \leq \frac{1}{2}\left[1 - s\left(\frac{\sum_{1\leq i\leq s} p(i)}{s}\right)^2\right] \\ =& \frac{1}{2}(1-\frac{1}{s}) \leq \frac{1}{2}(1-\frac{1}{r}).\end{aligned}$$

On the other hand,

$$\max_p f(p) \geq \frac{e(G)}{n^2}.$$

Combining, we have

$$e(G) \leq \frac{r-1}{2r} \cdot n^2.$$

∎

9.2 The Deleting Method

Previously, we often define an appropriate probability space and then show the random structure with desired property occurs with positive probability.

Today, we extend this idea and consider situation where random structure does not always have the desired property, and may have some very few "blemishes". The point that we want to make here is that after deleting all blemishes, we will obtain the wanted structure.

First we prove a half-way bound of Corollary 9.22.

Theorem 9.26. *Let G be a graph on n vertices and with average degree d. Then $\alpha(G) \geq \frac{n}{2d}$.*

Proof. Let $S \subset V(G)$ be a random subset, where for any $v \in V$, $P(v \in S) = p$. The value of p will be given later.

Let $X = |S|$ and $Y = e(S)$, Then $\mathbb{E}[X] = np$, $\mathbb{E}[Y] = mp^2$ where $m = \frac{nd}{2}$. So

$$\mathbb{E}[X - Y] = np - p^2 \cdot \frac{nd}{2} = n(p - \frac{d}{2}p^2).$$

By taking $p = \frac{1}{d}$, we have $\mathbb{E}[X - Y] = \frac{n}{2d}$. So there is a subset $S \subseteq V(G)$ such that $|S| - e(S) \geq \mathbb{E}[X - Y] = \frac{n}{2d}$. Now we delete one vertex for each edge of S. This leaves a subset $S^* \subseteq S$. Since all edges of S are destroyed, S^* must be an independent set of size at least $|S| - e(S) \geq \frac{n}{2d}$. ∎

Recall: If $\binom{n}{k}2^{1-\binom{k}{2}} < 1$, then Ramsey number $R(k,k) > n$. So $R(k,k) > \frac{1}{e\sqrt{2}}k2^{\frac{k}{2}}$.

Theorem 9.27. *For all n, $R(k,k) > n - \binom{n}{k}2^{1-\binom{k}{2}}$.*

Proof. Consider a random 2-edge-coloring of K_n, where each edge is colored by red or blue with probability $\frac{1}{2}$, independent of other choices. For $A \in \binom{[n]}{k}$, let X_A be the indicator random variable of the event that A induces a monochromatic K_k.

Let $X = \sum_{A \in \binom{[n]}{k}} X_A$ be the number of monochromatic k-subsets. Then we have

$$\mathbb{E}[X] = \sum_{A \in \binom{[n]}{k}} \mathbb{E}[X_A] = \binom{n}{k} 2^{1-\binom{k}{2}}.$$

So there exists a 2-edge-coloring of K_n, where the number of monochromatic k-subsets is at most $\mathbb{E}[X] = \binom{n}{k}2^{1-\binom{k}{2}}$. Next we remove one vertex from each monochromatic k-subset. This will delete at most $X \leq \binom{n}{k}2^{1-\binom{k}{2}}$ vertices and destroy all monochromatic k-subsets. So it remains at least $n - \binom{n}{k}2^{1-\binom{k}{2}}$ vertices, which contains NO monochromatic K_k. ∎

Corollary 9.28.

$$R(k,k) > \frac{1}{e}(1+o(1))k2^{\frac{k}{2}}.$$

Proof. Exercise, by maximizing $n - \binom{n}{k}2^{1-\binom{k}{2}}$ for a fixed k. ∎

9.3 Markov's Inequality

Theorem 9.29 (Markov's Inequality)**.** *Let $X \geq 0$ be a random variable and $t > 0$, then $P(X \geq t) \leq \frac{\mathbb{E}[X]}{t}$.*

Corollary 9.30. *Let $X_n \geq 0$ be integer value random variable for $n \in \mathbb{N}^+$ in (Ω_n, P_n). If $\mathbb{E}[X_n] \to 0$ as $n \to +\infty$, then $P(X_n = 0) \to 1$ (as $n \to +\infty$), i.e., $X_n = 0$ almost surely occurs.*

Theorem 9.31. *For a random graph $G(n,p)$ where $p \in (0,1)$, then*

$$P\left(\alpha(x) \leq \lceil \frac{2\ln n}{p} \rceil\right) \to 1 \quad as \quad n \to +\infty.$$

Proof. Let $k = \lceil \frac{2\ln n}{p} \rceil$. For any $S \in \binom{[n]}{k+1}$, let A_S be the event that S is an independent set, and let X_S be the indicator random variable of the event A_S. Let $X_n = \sum_{S \in \binom{[n]}{n+1}} X_S$ be the number of independent set of size $k+1$. Then $P(\alpha(G) \leq k) = P(X_n = 0)$. Now we compute $\mathbb{E}[X_n]$ as following:

$$\begin{aligned}
\mathbb{E}[X_n] = \sum_{S \in \binom{[n]}{k+1}} \mathbb{E}[X_S] &= \binom{n}{k+1}(1-p)^{\binom{k+1}{2}} \\
&\leq \frac{n^{k+1}}{(k+1)!} e^{-p\binom{k+1}{2}} \\
&= \frac{1}{(k+1)!}(ne^{-p\cdot\frac{k}{2}})^{k+1} \\
&\leq \frac{1}{(k+1)!} \to 0.
\end{aligned}$$

By the corollary, we see that $P(\alpha(G) \leq k) = P(X_n = 0) \to 1$ as $n \to +\infty$. ∎

Definition 9.32. *For a graph G, the* chromatic number $\chi(G)$ *is the minimum integer k such that $V(G)$ can be partitioned into k independent sets.*

Fact 9.33. *(1). $\chi(K_n) = n$,*
(2). $\chi(G) \leq 2$ if and only if G is bipartite,
(3). $\chi(C_{2n+1}) = 3$.

Proposition 9.34. *For any graph G on n vertices, $\chi(G) \cdot \alpha(G) \geq n$.*

Definition 9.35. *The girth $g(G)$ of a graph G is the length of a shortest cycle in G.*

Theorem 9.36 (Erdős)**.** *For any $k \in \mathbb{N}^+$, there exists a graph G with $\chi(G) \geq k$ and $g(G) \geq k$.*

Proof. Consider a random graph $G = G(n,p)$ where p will be determined later. Let $t = \lceil \frac{2 \ln n}{p} \rceil$, by the previous theorem, $\alpha(G) \leq t$ almost surely occurs.

Let X_n be the number of cycles of length less than k in G. Then

$$\mathbb{E}[X_n] = \sum_{i=3}^{k-1} \frac{n(n-1)\cdots(n-i+1)}{2i} \cdot p^i,$$

where $\frac{n(n-1)\cdots(n-i+1)}{2i}$ is the number of $C_i's$ in K_n. So

$$\mathbb{E}[X_n] \leq \sum_{i=3}^{k-1} (np)^i = \frac{(np)^k - 1}{np - 1}.$$

By Markov's inequality,

$$P(X_n > \frac{n}{2}) \leq \frac{E[X_n]}{n/2} \leq \frac{2[(np)^k - 1]}{n(np-1)}.$$

Let $p = n^{-\frac{k-1}{k}}$. So $np = n^{\frac{1}{k}}$. Then

$$P(X_n > \frac{n}{2}) \leq \frac{2(n-1)}{n(n^{\frac{1}{k}} - 1)} \to 0 \quad as \quad n \to +\infty.$$

So there exists a graph G on n vertices such that $X_n \leq n/2$ and $\alpha(G) \leq t = \lceil \frac{2 \ln n}{p} \rceil \leq 3 \ln n \cdot n^{\frac{k-1}{k}}$.

By deleting one vertex from each cycle of length at most $k-1$, we can find an induced subgraph G^* of G, which has at least $\frac{n}{2}$ vertices and NO cycles of length at most $k-1$. Moreover,

$$\alpha(G^*) \leq \alpha(G) \leq 3 \ln n \cdot n^{\frac{k-1}{k}}.$$

By Proposition 9.34, we have

$$\chi(G^*) \geq \frac{|V(G^*)|}{\alpha(G^*)} \geq \frac{n/2}{3(\ln n) n^{\frac{k-1}{k}}} \geq \frac{n^{1/k}}{6 \ln n} \geq k \text{ and } g(G^*) \geq k.$$

∎

10 The Algebraic Method

10.1 Odd/Even Town

Question 10.1. *A town has n residents. They want to form some clubs according to the following rules:*

(i) Each club has an odd number of members.

(ii) Every 2 clubs must share an even number of members.

How many clubs can they form?

Example 10.2. *(a)* $A_i = \{i\}$ *for* $i \in [n] \Rightarrow n$ *clubs.*

(b) n *is even,* $A_i = [n] \setminus \{i\} \Rightarrow n$ *clubs.*

(c) n *is even,* $A_1 = [n] \setminus \{1\}$, $A_2 = [n] \setminus \{2\}$, $A_i = \{1, 2, i\}$ *for* $i \in \{3, ..., n\} \Rightarrow n$ *clubs.*

Theorem 10.3 (Odd/Even town)**.** *Let* $\mathcal{F} \subseteq 2^{[n]}$ *be a family satisfying:*

(i) $|A|$ *is odd for all* $A \in \mathcal{F}$,

(ii) $|A \cap B|$ *is even, for all* $A \neq B \in \mathcal{F}$.

Then $|\mathcal{F}| \leq n$.

Proof. For each $A \in \mathcal{F}$, we define an indicator vector $\vec{\mathbb{1}}_A \in \mathbb{F}_2^n = \{0, 1\}^n$ such that

$$\vec{\mathbb{1}}_A(i) = \begin{cases} 1, & \text{if } i \in A, \\ 0, & \text{if } i \notin A, \end{cases}$$

where $\mathbb{F}_2$ is the finite field of size 2. Then, these conditions become

$$\begin{cases} \vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_A = 1, & \text{for any } A \in \mathcal{F}, \\ \vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_B = 0, & \text{for any } A \neq B \in \mathcal{F}. \end{cases}$$

Next, we claim that these vectors $\vec{\mathbb{1}}_A$ in $\mathbb{F}_2^n$ are linearly independent.
Let $\alpha_A \in \mathbb{F}_2$, such that $\sum_{A \in \mathcal{F}} \alpha_A \vec{\mathbb{1}}_A = \vec{0}$. Then for any $B \in \mathcal{F}$,

$$0 = \vec{0} \cdot \vec{\mathbb{1}}_B = (\sum_{A \in \mathcal{F}} \alpha_A \vec{\mathbb{1}}_A) \cdot \vec{\mathbb{1}}_B = \sum_{A \in \mathcal{F}} \alpha_A (\vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_B) = \alpha_B \cdot \vec{\mathbb{1}}_B \cdot \vec{\mathbb{1}}_B = \alpha_B.$$

This proves the claim. Therefore the number of vectors $\vec{\mathbb{1}}_A$'s is at most the dimension of $\mathbb{F}_2^n$, which is n. So $|\mathcal{F}| \leq n$. ∎

10.2 Even/Odd Town

Theorem 10.4 (Even/Odd town). *Let $\mathcal{F} \subseteq 2^n$ be such that:*

(i) $|A|$ is even, for all $A \in \mathcal{F}$,

(ii) $|A \cap B|$ is odd, for all $A \neq B \in \mathcal{F}$.

Then $|\mathcal{F}| \leq n$.

First we show a weaker result:

Lemma 10.5. *Such $\mathcal{F}$ satisfies $|\mathcal{F}| \leq n+1$.*

Proof. Adding a new element $n+1$ to each set $A \in \mathcal{F}$ to get a new family $\mathcal{F}^*$. We see $\mathcal{F}^*$ satisfies the Odd/Even town conditions. So $|\mathcal{F}| = |\mathcal{F}^*| \leq n+1$. ∎

Now we give the proof of Theorem 10.4.

Proof of Theorem 10.4. It suffices to prove that $|\mathcal{F}| \neq n+1$. Suppose for a contradiction that $\mathcal{F} = \{A_1, A_2, \cdots, A_{n+1}\}$. For each $A_i \in \mathcal{F}$, define $\vec{\mathbb{1}}_{A_i} \in \mathbb{F}_2^n$ as before. So we have $n+1$ vectors in an n-dimension space. Thus, they must be linearly dependent. Therefore, there exist $\alpha_i \in \mathbb{F}_2$ for $1 \leq i \leq n+1$ which are not all 0's such that

$$\sum_{i=1}^{n+1} \alpha_i \vec{\mathbb{1}}_{A_i} = \vec{0}.$$

We also have

$$\begin{cases} \vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_A = 0, & \text{for any } A \in \mathcal{F} \\ \vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_B = 1, & \text{for any } A \neq B \in \mathcal{F}. \end{cases}$$

Then for each $1 \leq j \leq n+1$,

$$0 = \vec{0} \cdot \vec{\mathbb{1}}_{A_j} = \left(\sum_{i=1}^{n+1} \alpha_i \vec{\mathbb{1}}_{A_i} \right) \cdot \vec{\mathbb{1}}_{A_j} = \sum_{i=1}^{n+1} \alpha_i - \alpha_j.$$

So $\alpha_j = \sum_{i=1}^{n+1} \alpha_i$ for all $1 \leq j \leq n+1$. They are all equal. Because all α_j's can not be all 0's, we derive that $\alpha_j = 1$ for all $1 \leq j \leq n+1$ and n must be even. Moreover,

$$\sum_{i=1}^{n+1} \vec{\mathbb{1}}_{A_i} = \vec{0}. \tag{10.10}$$

Consider $\mathcal{F}^c = \{A^c : A \in \mathcal{F}\}$, we will see that $\mathcal{F}^c$ also satisfies the Even/Odd town conditions:

- $|A^c| = n - |A|$ is even, for all $A \in \mathcal{F}$.
- $|A^c \cap B^c| = n - |A \cup B| = n - |A| - |B| + |A \cap B|$ is odd, for all $A \neq B \in \mathcal{F}$.

By the same proof, we can derive that

$$\sum_{i=1}^{n+1} \vec{\mathbb{1}}_{A_i^c} = \vec{0}. \tag{10.11}$$

Now (10.10)+(10.11) gives that

$$\vec{0} = \sum_{i=1}^{n+1} (\vec{\mathbb{1}}_{A_i} + \vec{\mathbb{1}}_{A_i^c}) = (n+1)\vec{1} = \vec{1},$$

a contradiction. ∎

Example 10.6 (Even/Even-town). *Let $\mathcal{F} \subset 2^{[n]}$ be such that:*

(i) $|A|$ =even, for all $A \in \mathcal{F}$,

(ii) $|A \cap B|$ =even, for all $A \neq B \in \mathcal{F}$.

Then $|\mathcal{F}| \leq 2^{n/2}$. (let n be even)

10.3 Fisher's Inequality

Theorem 10.7 (Fisher's Inequality). *For a fixed k, let $\mathcal{F} \subseteq 2^{[n]}$ be a family such that $|A \cap B| = k$, for all $A \neq B \in \mathcal{F}$. Then, $|\mathcal{F}| \leq n$.*

Proof. For each $A \in \mathcal{F}$, define vector $\vec{\mathbb{1}}_A \in R^n$ as before. Then for any $A, B \in \mathcal{F}$, $\vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_B = k$. Again, we want to show $\vec{\mathbb{1}}_A$'s are linearly independent over $\mathbb{R}^n$. Let $\sum_{A \in \mathcal{F}} \alpha_A \vec{\mathbb{1}}_A = \vec{0}$, where $\alpha_A \in \mathbb{R}$. Then

$$0 = \left(\sum_{A \in \mathcal{F}} \alpha_A \vec{\mathbb{1}}_A\right) \cdot \left(\sum_{A \in \mathcal{F}} \alpha_A \vec{\mathbb{1}}_A\right) = \sum_{A \in \mathcal{F}} \alpha_A^2 \vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_A + \sum_{A \neq B} \alpha_A \alpha_B \vec{\mathbb{1}}_A \cdot \vec{\mathbb{1}}_B$$

$$= \sum_{A \in \mathcal{F}} \alpha_A^2 |A| + k \cdot \sum_{A \neq B} \alpha_A \alpha_B = k \left(\sum_{A \in \mathcal{F}} \alpha_A\right)^2 + \sum_{A \in \mathcal{F}} \alpha_A^2 (|A| - k) \geq 0,$$

where the last inequality holds because each A is of size at least k. This implies that $\sum_{A \in \mathcal{F}} \alpha_A = 0$ and $\alpha_A^2(|A| - k) = 0$ for all $A \in \mathcal{F}$. Since $|A \cap B| = k$ for any $A \neq B \in \mathcal{F}$, we have at most one set A of size exactly k. Call this subset A^* if exists. Thus for each $A \in \mathcal{F} \setminus \{A^*\}$, $\alpha_A = 0$. However $\sum_{A \in \mathcal{F}} \alpha_A = 0$, we derive that all $\alpha_A = 0$. Thus all $\vec{\mathbb{1}}_A$'s are independent and then $|\mathcal{F}| \leq n$. ∎

Lemma 10.8. *Suppose P is a set of n points in $\mathbb{R}^2$. Then either they are in a line, or they define at least n lines.*

Proof. Let L be the family of all lines defined by P. We want to show that $|L| = 1$ or $|L| \geq n$ For each point $x_i \in P$, define $L_i = \{\ell \in L : \text{the line } \ell \text{ passes through } x_i\}$. Note that for all $i \neq j$, $|L_i \cap L_j| = 1$. We also observe that there exist $i \neq j$ with $L_i = L_j$ if and only if all n points lie in a line. Therefore, either $|L| = 1$, or for any $x_i, x_j \in P$, we have $L_i \neq L_j$. We may assume that the second case occurs. Let $\mathcal{F} = \{L_i : x_i \in P\}$. Clearly, $\mathcal{F}$ satisfies the conditions of Fisher's inequality, so we can derive that $n = |\mathcal{F}| \leq |L|$. ∎

Lemma 10.9. *Let G be a graph whose vertices are triples in $\binom{[k]}{3}$ such that for any two $A, B \in \binom{[k]}{3}$, $A \sim_G B$ if and only if $|A \cap B| = 1$. Then G doesn't contain any clique or independent set of size k+1.*

Proof. Consider the maximum clique of G, say using vertices $A_1, A_2, ..., A_m \in \binom{[k]}{3}$ with $|A_i \cap A_j| = 1$, for $1 \leq i < j \leq m$. By Fisher's inequality, $m \leq k$.

Now consider the maximum independent set of G, say consisting of vertices $B_1, B_2, ..., B_t \in \binom{[k]}{3}$. We see $|B_i| = 3$ is odd and $|B_i \cap B_j| = 0$ or 2 is even. By Odd/Even-town, we have $t \leq k$. ∎

Corollary 10.10. $R(k+1, k+1) > \binom{k}{3}$.

Remark 10.11. *This gives us an explicit construction for Ramsey number $R(k+1, k+1)$.*

Note that this bound is much weaker than previous bound $R(k+1, k+1) > c \cdot k2^{\frac{k}{2}}$.

10.4 1-Distance Problem

Problem 10.12 (1-Distance Problem)**.** *Given n points in $\mathbb{R}^2$, what is the maximum number of pairs of distance 1?*

Theorem 10.13. *There are at most $O(n^{\frac{3}{2}})$ pairs at distance 1.*

Proof. Define a graph G on n points as following: for points a, b, $a \sim b$ if and only if $d(a, b) = 1$.

We claim that G is $K_{2,3}$-free. Since the neighbors of the point a must lie on the circle with center a and with radius 1, and any such 2 circles can intersect at most 2 points, then they show that G is $K_{2,3}$-free.

Thus the number of pairs at distance 1 is

$$e(G) \leq \text{ex}(n, K_{2,3}) = O(n^{\frac{3}{2}}).$$

∎

Example 10.14.

$$\text{ex}(n, K_{2,3}) = O(n^{\frac{3}{2}}).$$

Open problem (Erdős)**.** *Can one find an example of n points in $\mathbb{R}^2$ with n^{1+c} pairs at distance 1 for $c > 0$?*

Problem 10.15. *What is the maximum number of points in $\mathbb{R}^n$ such that the distance between any two points is 1?*

Theorem 10.16. *There are at most $n+1$ points in $\mathbb{R}^n$ such that the distance between any two points is 1.*

Proof. Assume we have $m+1$ such points in $\mathbb{R}^n$. We assume one of them is $\vec{0}$ and let others be $\vec{v_1}, \vec{v_2}, ..., \vec{v_m} \in \mathbb{R}^n$. Then we have

- $\vec{v_i} \cdot \vec{v_i} = ||\vec{v_i} - \vec{0}||^2 = 1$ for $i \in [m]$,
- $\vec{v_i} \cdot \vec{v_j} = \frac{1}{2}$, for any $i \neq j \in [m]$,

because $1 = ||\vec{v_i} - \vec{v_j}||^2 = ||\vec{v_i}||^2 + ||\vec{v_j}||^2 - 2\vec{v_i} \cdot \vec{v_j} = 1 + 1 - 2\vec{v_i} \cdot \vec{v_j}$.

Consider the matrix

$$A = \begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_m \end{pmatrix}_{m \times n}.$$

So

$$A \cdot A^T = \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{2} \\ \frac{1}{2} & 1 & \cdots & \frac{1}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2} & \frac{1}{2} & \cdots & 1 \end{pmatrix}_{m \times m}.$$

Since $\det(A \cdot A^T) \neq 0$, we get $\text{rank}(A \cdot A^T) = m$. Then $n \geq \text{rank } A \geq \text{rank}(A \cdot A^T) = m$. So $m \leq n$ as desired. ∎

Remark: we can also apply this method for the Even/Odd town problem.

Definition 10.17. *A* <u>*2-distance set*</u> *is a set of points in $\mathbb{R}^n$ whose pairwise distance is either c or d for some $c, d > 0$.*

Problem 10.18 (2-Distance Problem)**.** *What is the maximum size of a 2-distance set?*

In the previous approach, we define a vector $\vec{1}_A$ for each $A \in \mathcal{F}$. Instead of considering vectors, one also can define certain polynomials, as polynomials of certain degree also form a vector space.

Lemma 10.19. *For $i \in [n]$, let $f_i : \Omega \to \mathbb{F}$ be polynomial, where $\mathbb{F}$ is a field. If there are elements $v_i \in \Omega$ for $i \in [n]$ satisfying*

$$\begin{cases} f_i(v_i) \neq 0, & \text{for any } i \in [n] \\ f_i(v_j) = 0, & \text{for any } j < i, \end{cases}$$

then $f_1, f_2, ..., f_n$ are linear independent over the "linear space" spanned by polynomials $f : \Omega \to \mathbb{F}$.

Proof. Exercise. ∎

Theorem 10.20. *Any 2-distance set in $\mathbb{R}^n$ has at most $\frac{1}{2}(n+1)(n+4)$ points.*

Proof. Let $A = \{\vec{a}_1, \vec{a}_2, ..., \vec{a}_m\}$ be such a set with distances $c > 0$, $d > 0$. For each $i \in [m]$, define $f_i(\vec{x}) = (||\vec{x} - \vec{a}_i||^2 - c^2)(||\vec{x} - \vec{a}_i||^2 - d^2)$ for $\vec{x} \in \mathbb{R}^n$. Then

$$\begin{cases} f_i(\vec{a}_i) = c^2 d^2 \neq 0, & \text{for any } i \\ f_i(\vec{a}_j) = (||\vec{a}_j - \vec{a}_i||^2 - c^2)(||\vec{a}_j - \vec{a}_i||^2 - d^2) = 0, & \text{for any } j \neq i. \end{cases}$$

By Lemma 10.19, $f_1, f_2, ..., f_m$ are linearly independent in the "linear space" that contains $f_1, ..., f_m$. We want to bound the dimension of "some vector space" which contains all polynomials $f_1, f_2, ..., f_m$.

Let $\vec{x} = (x_1, x_2, ..., x_n), \vec{a}_i = (a_{i1}, ..., a_{in})$. Note that

$$\begin{aligned} f_j(\vec{x}) &= (\sum_i (x_i - a_{ji})^2 - c^2)(\sum_i (x_i - a_{ji})^2 - d^2) \\ &= (\sum_i x_i^2 - 2\sum_i x_i a_{ji} + \sum_i a_{ji}^2 - c^2)(\sum_i x_i^2 - 2\sum_i x_i a_{ji} + \sum_i a_{ji}^2 - d^2), \end{aligned}$$

can be expressed as the linear combination of the following polynomials:

$$B = \{(\sum_i x_i^2)^2, x_j(\sum_i x_i^2), x_i x_j, x_i, 1\}.$$

We see that B contains $1 + n + \binom{n}{2} + n + n + 1 = \frac{n(n-1)}{2} + 3n + 2 = \frac{(n+1)(n+4)}{2}$ elements and each f_i is contained in the linear space spanned by B. So $|A| = m$ is at most the dimension of $span(B)$, which is at most $\frac{(n+1)(n+4)}{2}$.

∎

Remark 10.21. *This proof can be extended to k-distance Problem.*

Next, we consider a generalization of Fisher's inequality.

Definition 10.22. *Consider a subset $L \subseteq \{0, 1, 2, ..., n\}$. We say a family $\mathcal{F} \subseteq 2^{[n]}$ is L-intersecting, if for any $A \neq B \in \mathcal{F}$, $|A \cap B| \in L$.*

Theorem 10.23 (Frankl-Wilson, 1981)**.** *If $\mathcal{F} \subseteq 2^{[n]}$ is an L-intersecting family, then $|\mathcal{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}$.*

Proof. Let $\mathcal{F} = \{A_1, A_2, ..., A_m\}$ where $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. For each $i \in [m]$, define $f_i(\vec{x}) : \mathbb{R}^n \to \mathbb{R}^n$ by

$$f_i(\vec{x}) = \prod_{\ell \in L, \ell < |A_i|} (\vec{x} \cdot \vec{1}_{A_i} - \ell).$$

Consider the indicator vectors $\vec{1}_{A_1}, \vec{1}_{A_2}, ..., \vec{1}_{A_m}$. Then we have

- $f_i(\vec{1}_{A_i}) = \prod_{\ell \in L, \ell < |A_i|}(|A_i| - \ell) > 0$, for any $i \in [n]$,
- $f_i(\vec{1}_{A_j}) = \prod_{\ell \in L, \ell < |A_i|}(|A_i \cap A_j| - \ell) = 0$, for all $j < i$.

This is because we have $\ell = |A_j \cap A_i| \in L$ and $\ell < |A_i|$ for some ℓ (as $j < i$, $|A_j| \leq |A_i|$). By Lemma 10.19, we see that $f_1, f_2, ..., f_m$ are linear independent.

Next we want to define some new polynomials $\tilde{f}_i(\vec{x})$ from f_i such that $\tilde{f}_1, \tilde{f}_2, ..., \tilde{f}_m$ are remain linearly independent, but these $\tilde{f}_i(\vec{x})$'s lie in a "better" linear space.

Observer that all vector $\vec{1_{A_j}}$ are 0/1-vectors. Let $\tilde{f}_i(\vec{x})$ be a new polynomial obtained from $f_i(\vec{x})$ by replacing all terms x_j^k (for $k \geq 1$) by x_j.

For any 0/1-vectors $\vec{y}$, we have $\tilde{f}_i(\vec{y}) = f_i(\vec{y})$. This shows that $\tilde{f}_1, \tilde{f}_2, ..., \tilde{f}_m$ are also linearly independent. And we see each $\tilde{f}_i(\vec{x})$ is a linear combination of the monomials $\prod_{i \in I} x_i$ for $I \in [n]$ with $|I| \leqslant |L|$ (as $\deg \tilde{f}_i \leq \deg f_i \leq |L|$). Clearly the number of such monomials is at most $\sum_{k=0}^{|L|} \binom{n}{k}$ which is also the dimension of the space containing $\tilde{f}_1, \tilde{f}_2, ..., \tilde{f}_m$. This prove that

$$|\mathcal{F}| = |m| \leq \sum_{k=0}^{|L|} \binom{n}{k}.$$

∎

Theorem 10.24. *Let p be a prime and $L \subseteq \mathbb{F}_p = \{0, 1, ..., p-1\}$. Let $\mathcal{F} \subseteq 2^{[n]}$ be a family satisfying that*

- $|A| \notin L \pmod p$ *for any* $A \in \mathcal{F}$,
- $|A \cap B| \in L \pmod p$ *for all* $A \neq B \in \mathcal{F}$.

Then $|\mathcal{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}$.

Proof. All operations are mod p. Let $\mathcal{F} = \{A_1, ..., A_m\}$. Define $f_i(\vec{x}) : \mathbb{F}_p^* \to \mathbb{F}_p$ be such that

$$f_i(\vec{x}) = \prod_{\ell \in L} (\vec{x} \cdot \vec{1}_{A_i} - \ell).$$

Then

- $f_i(\vec{1}_{A_i}) = \prod_{\ell \in L}(|A_i| - \ell) \neq 0$, for any $i \in [n]$,
- $f_i(\vec{1}_{A_j}) = \prod_{\ell \in L}(|A_i \cap A_j| - \ell) = 0$ for all $i \neq j$.

So $f_1, f_2, ..., f_m$ are linearly independent over Z_p^n. Then repeating the proof of Theorem 10.23, we get the desired bound. ∎

Now we prove an application of these results.

Theorem 10.25 (Frankl-Wilson)**.** *For any prime* p*, there is a graph* G *on* $n = \binom{p^3}{p^2-1}$ *vertices such that both of the maximum clique and the maximum independent set are at most* $\sum\limits_{i=0}^{p-1} \binom{p^3}{i}$.

Proof. Let $G = (V, E)$ be the following graph, where $V = \binom{[p^3]}{p^2-1}$, and for $A, B \in V$, $A \sim_G B$ if and only if $|A \cap B| \not\equiv p - 1 \pmod p$.

Consider the maximum clique with vertex $A_1, A_2, ..., A_m \in \binom{[p^3]}{p^2-1}$. Thus we have

- $|A_i \cap A_j| \not\equiv p - 1 \pmod p$, for all $i \neq j$,
- $|A_i| = p^2 - 1 \equiv p - 1 \pmod p$, for any $i \in [n]$.

By Theorem 10.24 with $L = \{0, 1, 2, ..., p-2\} \subseteq \mathbb{F}_p$ we can derive that $m \leqslant \sum\limits_{i=0}^{p-1} \binom{p^3}{i}$.

Consider the maximum independent set $B_1, B_2, ..., B_t$. Then we have $|B_i \cap B_j| = p-1 \pmod p$ for all $i \neq j$, implying that $|B_i \cap B_j| \in \{p-1, 2p-1, ..., p(p-1)-1\} = L^*$ with $|L^*| = p-1$. Thus $B_1, B_2, ..., B_t$ is L^*-intersecting family in $\binom{[p^3]}{p^2-1}$. By Theorem 10.23, we have $t \leqslant \sum_{i=0}^{p-1} \binom{p^3}{i}$. ∎

Corollary 10.26.

$$R(k+1, k+1) \geq k^{\Omega(\log(k)/\log(\log(k)))}.$$

Proof. Use the construction from Theorem 10.25. Let $k = \sum_{i=0}^{p-1} \binom{p^3}{i}$. So $R(k+1, k+1) > n$. We have that

$$k = \sum_{i=0}^{p-1} \binom{p^3}{i} \simeq \binom{p^3}{p} \simeq (p^2)^p \simeq p^{2p}, \; n \simeq (\frac{p^3}{p^2})^{p^2} \simeq p^{p^2},$$

which implies that

$$\log(k) \simeq p \log(p), \; \log(\log(k)) \simeq \log(p),$$

so

$$p \simeq \frac{\log(k)}{\log(\log(k))}.$$

Then we have

$$n = \binom{p^3}{p^2-1} \simeq (p^{2p})^{p/2} \simeq k^p = k^{\Omega(\log(k)/\log(\log(k)))}.$$

∎

Definition 10.27. *Given a set $S \subseteq R^n$, the* diameter *of S is defined as $Diam(S) = \sup\{d(x,y) : x, y \in S\}$ where $d(x,y)$ denotes the Euclidean distance between x and y in R^n.*

If $Diam(S) < +\infty$, then we say S is bounded.
Borswk's Conjecture: Every bounded $S \subseteq R^d$ can be partitioned into $d+1$ sets of strictly smaller diameter.

Remark 10.28. *This was verified for all $S \subseteq R^d$ with $d \leqslant 3$ and for the S is a sphere and any $d \geq 2$.*

Lemma 10.29. *For any prime p, there is a set $\mathcal{F}$ of $\frac{1}{2}\binom{4p}{2p}$ vectors in $\{-1,1\}^{4p}$ such that every subset of size $2\binom{4p}{p-1}$ vectors contains an orthogonal pair of vectors.*

Proof. Let Q=$\{I \in \binom{[4p]}{2p} : 1 \in I\}$, then $|Q| = \frac{1}{2}\binom{4p}{2p}$. For any $I \in Q$, define $\vec{v}^I \in \{-1,1\}^{4p}$ by

$$\vec{v}^I_i = \begin{cases} 1, & i \in I \\ -1, i \notin I. \end{cases}$$

Let $\mathcal{F} = \{\vec{v}^I : I \in Q\}$ with $|\mathcal{F}| = |Q| = \frac{1}{2}\binom{4p}{2p}$.
Claim 1. $\vec{v}^I \perp \vec{v}^J$ if and only if $|I \cap J| \equiv 0 \pmod p$.

Proof. $\vec{v}^I \perp \vec{v}^J$ if and only if $\vec{v}^I \cdot \vec{v}^J = 0$. Since $\vec{v}^I \cdot \vec{v}^J = |I \cap J| - |I^C \cap J| - |I \cap J^C| + |I^C \cap J^C|$ (we have $|I \cap J| = |I^C \cap J^C|$ as $|I| = |J| = 2p$), we have that $\vec{v}^I \perp \vec{v}^J$ if and only if $|I \Delta J| = 2p = 4p - 2|I \cap J|$ if and only if $|I \cap J| = p$

Since $1 \in I \cap J$ and $|I| = |J| = 2p$, we have $\vec{v}^I \perp \vec{v}^J$ if and only if $|I \cap J| \equiv 0 \pmod p$. ∎

Claim 2. For any subset $\mathcal{F}' \subseteq \mathcal{F}$ without orthogonal pairs, $|\mathcal{F}'| \leq \sum_{k=0}^{p-1}\binom{4p}{k} < 2\binom{4p}{p-1}$.

Proof. Let $Q' = \{I \in Q : \vec{v}^I \in \mathcal{F}'\}$. By Claim 1, Q' is a subfamily of $\binom{[4p]}{2p}$ satisfying

- $|A| = 2p \equiv 0 \pmod p$, for any $A \in Q'$,
- $|A \cap B| \neq 0 \pmod p$, for any $A \neq B \in Q'$.

By Theorem 10.25 (with $L = \{1, 2, ..., p-1\}$), we get $|\mathcal{F}'| = |Q'| \leq \sum_{k=0}^{p-1}\binom{4p}{k}$. ∎

Now the conclusion of Lemma follows by Claim 2. ∎

Definition 10.30. *The* tensor product *of a vectors $\vec{v} \in \mathbb{R}^n$ is $\vec{w} = \vec{v} \otimes \vec{v} \in \mathbb{R}^{n^2}$ by $w_{ij} = v_i \cdot v_j$ for all $1 \leq i, j \leq n$.*

Theorem 10.31 (Kahn-Kalai, 1993)**.** *For sufficiently large d, there exists a bounded set $S \subset \mathbb{R}^d$(a finite set) such that any partition of S into $1.1^{\sqrt{d}}$ subsets contains a subset of the same diameter.*

Proof. Take the family $\mathcal{F}$ from the above lemma. So $\mathcal{F} \subset \{-1,1\}^n \subset \mathbb{R}^n$ (with $n = 4p$). Let $X = \{\vec{v} \otimes \vec{v} : \vec{v} \in \mathcal{F}\} \subseteq \mathbb{R}^{n^2}$. Let $d = n^2 = (4p)^2 = 16p^2$. For any $\vec{w} = \vec{v} \otimes \vec{v} \in X$,

$$||\vec{w}||^2 = \sum_{1 \le i,j \le n} w_{ij}^2 = \sum_{1 \le i,j \le n} v_i^2 v_j^2 = (\sum_{i=1}^{n} v_i^2)(\sum_{j=1}^{n} v_j^2) = n^2,$$

and thus $||\vec{w}|| = n$.

For $\vec{w} = \vec{v} \otimes \vec{v}, \vec{w}' = \vec{v}' \otimes \vec{v}' \in X$, we have

$$\vec{w} \cdot \vec{w}' = \sum_{1 \le i,j \le n} w_{ij} w'_{ij} = \sum_{1 \le i,j \le n} (v_i v'_i)(v_j v'_j) = (\sum v_i v'_i)^2 = (\vec{v} \cdot \vec{v}')^2.$$

This says that $\vec{w} \perp \vec{w}'$ if and only if $\vec{v} \perp \vec{v}'$. Thus,

$$||\vec{w} - \vec{w}'||^2 = ||\vec{w}||^2 + ||\vec{w}'||^2 - 2\vec{w} \cdot \vec{w}' = 2n^2 - 2(\vec{v} \cdot \vec{v}')^2 \le 2n^2,$$

this proves that $Diam(X) = \sqrt{2}n$ and $|X| = |\mathcal{F}| = \frac{1}{2}\binom{[4p]}{2p}$.

By Lemma 10.29, any subset of $2\binom{4p}{p-1}$ vectors in $\mathcal{F}$ contains an orthogonal pair of vector $\vec{v}, \vec{v}'$. Thus, any subset of $2\binom{4p}{p-1}$ vectors in X must contain a pair $\vec{w} = \vec{v} \otimes \vec{v}, \vec{w}' = \vec{v}' \otimes \vec{v}'$ with $\vec{v} \perp \vec{v}'$, which give the maximum distance $||\vec{w} - \vec{w}'|| = \sqrt{2}n$. Thus to decrease the diameter, we must partition X into subsets of size less than $2\binom{4p}{p-1}$, so the number of subsets needed is at least

$$\frac{|X|}{2\binom{4p}{p-1}} = \frac{\frac{1}{2}\binom{4p}{2p}}{2\binom{4p}{p-1}} = \frac{1}{4}\frac{(3p+1)\cdots(2p+1)}{(2p)\cdots(p)} \ge \frac{1}{4} \cdot (\frac{3}{2})^{p+1} \ge C \cdot (\frac{3}{2})^{\frac{\sqrt{d}}{4}} \ge 1.1^{\sqrt{d}},$$

where $d = n^2 = 16p^2$ is the dimension of X. ∎

10.5 Bollobás' Theorem

We first recall the following theorem which we learned in Chapter 3.2.

Sperner's Theorem: Let $\mathcal{F} \subseteq 2^{[n]}$ be a family such that for any $A \ne B \in \mathcal{F}$, $A \not\subseteq B$, and $B \not\subseteq A$, then $|\mathcal{F}| \le \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

LYM-inequality: For such $\mathcal{F}$, $\sum\limits_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \le 1$.

Theorem 10.32 (Bollobás' Theorem)**.** *Let $A_1, A_2, ..., A_m$ and $B_1, B_2, ..., B_m$ be the subsets of some ground set Ω. If we have*

(1) $A_i \cap B_j \ne \emptyset$, for any $i \ne j \in [m]$,

(2) $A_i \cap B_i = \emptyset$, for any $i \in [m]$.

Then $\sum\limits_{i=1}^{m} \frac{1}{\binom{a_i+b_i}{a_i}} \le 1$, where $a_i = |A_i|$ and $b_j = |B_j|$.

Remark 10.33. *The condition (1): $A_i \cap B_j \neq \emptyset$, for any $i \neq j$ cannot be weakened to $i < j$; otherwise we have the following counterexamples:*

- $m = 2$, $A_1 = B_2 = \{1\}$ *and* $A_2 = B_1 = \emptyset$.

  We can see that $\sum_{i=1}^{m} \frac{1}{\binom{a_i+b_i}{a_i}} = 2 > 1$.

- $m = 3$, $A_1 = B_2 = \{1\}$, $A_2 = A_3 = B_1 = \{3\}$, *and* $B_3 = \{1, 2\}$.

  We can see that $\sum_{i=1}^{m} \frac{1}{\binom{a_i+b_i}{a_i}} = \frac{4}{3} > 1$.

Proposition 10.34. *Bollobás' Theorem can imply LYM-inequality and LYM-inequality will imply Sperner's Theorem.*

Proof. We first show that Bollobás' Theorem can imply the LYM-inequality. Let $\mathcal{F} \subseteq 2^{[n]}$ satisfy that $A \not\subseteq B$, and $B \not\subseteq A$ for any $A \neq B \in \mathcal{F}$. Let $\mathcal{F} = \{A_1, A_2, ..., A_m\}$ and $\mathcal{F}' = \{B_1, B_2, ..., B_m\}$, where $B_i = [n] \backslash A_i$. We now varify that $A_1, ..., A_m$ and $B_1, ..., B_m$ satisfy the conditions (1) and (2).

- $A_i \cap B_j = A_i \backslash A_j \neq \emptyset$, for any $i \neq j \in [m]$,
- $A_i \cap B_i = \emptyset$, for any $i \in [m]$.

So by Bollobás' Theorem:

$$1 \geq \sum_{i=1}^{m} \frac{1}{\binom{a_i+b_i}{a_i}} = \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A_i|}}.$$

Note that LYM-inequality can easily imply the Sperner's Theorem and we are done. ∎

Proof of Bollobás' Theorem. Let $X = \bigcup_{i=1}^{m} (A_i \cup B_i)$ and let $n = |X|$. We will prove by induction on n. Base case: $n = 1$ ($A_1 = \{1\}, B_1 = \emptyset$) is clear.

Now we assume this statement holds for $|X| \leq n - 1$. Let $I_x = \{i \in [m] : x \notin A_i\}$ for any $x \in X$. Define $\mathcal{F}_x = \{A_i : i \in I_x\} \cup \{B_i \backslash \{x\} : i \in I_x\}$. Since each set in $\mathcal{F}_x$ doesn't contain x, we see that $|\cup_{S \in \mathcal{F}_x} S| \leq |X \setminus \{x\}| \leq n - 1$. Moreover, the family $\mathcal{F}_x$ satisfy the induction hypothesis. Hence by induction, we get

$$\sum_{i \in I_x} \frac{1}{\binom{|A_i| + |B_i \backslash \{x\}|}{|A_i|}} \leq 1, \text{ for any } x \in X.$$

We sum up the above inequalities for all $x \in X$ and get

$$\sum_{x \in X} \sum_{i \in I_x} \frac{1}{\binom{|A_i| + |B_i \backslash \{x\}|}{|A_i|}} \leq n. \tag{10.12}$$

For each $i \in [m]$, it contributes either 0, or $\frac{1}{\binom{a_i+b_i}{a_i}}$ or $\frac{1}{\binom{a_i+b_i-1}{a_i}}$ to each x. The term $\frac{1}{\binom{a_i+b_i}{a_i}}$ occurs when $i \in I_x$ and $x \notin B_i$, i.e., $x \notin A_i \cup B_i$ which occur exactly $(n - a_i - b_i)$ times. The term

$\frac{1}{\binom{a_i+b_i-1}{a_i}}$ occurs when $i \in I_x$ and $x \in B_i$, i.e., $x \in B_i$ which occur exactly b_i times. Therefore, we see that (10.12) is equivalent to

$$\sum_{i=1}^{m}\left((n-a_i-b_i)\frac{1}{\binom{a_i+b_i}{a_i}}+b_i\frac{1}{\binom{a_i+b_i-1}{a_i}}\right)\le n.$$

Since we have $\frac{1}{\binom{a_i+b_i-1}{a_i}}=\frac{1}{\binom{a_i+b_i}{a_i}}\cdot\frac{a_i+b_i}{b_i}$, which implies that

$$n\sum_{i=1}^{m}\frac{1}{\binom{a_i+b_i}{a_i}}\le n,$$

as claimed. ∎

Definition 10.35. *Let $\mathbb{F}$ be a field. A set $A \subseteq \mathbb{F}^n$ is in general position, if any n vectors in A are linearly independent over $\mathbb{F}$.*

Example 10.36. *For $a \in \mathbb{F}$, let $\vec{m}(a) = (1, a, a^2, ..., a^{n-1}) \in \mathbb{F}^n$ be a moment curve. Then $\{\vec{m}(a) : a \in \mathbb{F}\}$ is in general position (because of the Vandermonde matrix).*

Next, we use the so-called "general position" argument to prove the skew version of Bollobás' Theorem, where the condition (1) is relaxed to $i < j$.

Theorem 10.37. *(The skew version of Bollobás' Theorem) Let $A_1, ..., A_m$ be the sets of size r and $B_1, ..., B_m$ be the sets of size s such that*

- *$A_i \cap B_j \neq \emptyset$, for any $i < j$,*
- *$A_i \cap B_i = \emptyset$, for any $i \in [m]$.*

Then $m \le \binom{r+s}{s}$.

Proof. Let X=$\bigcup_{i\in[m]}(A_i \cup B_i)$. Take a set V of vectors $\vec{v} = (v_0, v_1, ..., v_r)$ in $\mathbb{R}^{r+1}$ such that V is in general position and $|V| = |X|$. Then we identify the elements of X with vectors of V. From now on, we may view each A_i or B_j as a subset in $V \subseteq \mathbb{R}^{r+1}$, where $|A_i| = r$ and $|B_j| = s$. For each $j \in [m]$, we define $f_j(\vec{x}) = \prod_{\vec{v}\in B_j} \vec{x}\cdot\vec{v}$ for any $\vec{x} \in \mathbb{R}^{r+1}$. So

$$f_j(\vec{x}) = \prod_{\substack{\vec{v}=(v_0,...,v_r)\\ \vec{v}\in B_j}} (v_0x_0 + \cdots + v_rx_r),$$

where $\vec{x} = (x_0, ..., x_r) \in \mathbb{R}^{r+1}$. Note that $f_j(\vec{x})$ is generated by the following monomials $x_0^{i_0}x_1^{i_1}\cdots x_r^{i_r}$, where $i_0 + i_1 + \cdots + i_r = s$ and $i_j \ge 0$ for $0 \le j \le r$. There are exactly $\binom{s+r}{r}$ such monomials, so $f_1, f_2, .., f_m$ are contained in a polynomial linear space of dimension $\binom{s+r}{r}$. It suffices to prove that $f_1, f_2, .., f_m$ are linearly independent. Note that

$$f_j(\vec{x}) = 0 \text{ if and only if there exists some } \vec{v} \in B_j \text{ such that } \vec{v}\cdot\vec{x} = 0. \tag{10.13}$$

Consider the linear subspace Span(A_i), which is spanned by the r vectors in A_i. Since $A_i \subseteq V \subseteq \mathbb{R}^{r+1}$ and V is in general position, we see that all r vectors in A_i are linearly independent and thus $dim\big(Span(A_i)\big) = r$. So $(Span(A_i))^{\perp}$ has dimension 1. We choose $\vec{a}_i \in (Span(A_i))^{\perp}$ for each $i \in [m]$. Then for each $\vec{v} \in V$,

$$\vec{v} \cdot \vec{a}_i = 0 \text{ if and only if } \vec{v} \in Span(A_i) \text{ if and only if } \vec{v} \in A_i. \tag{10.14}$$

Because, otherwise the $r+1$ vectors in $\{\vec{v}\} \cup A_i$ are linearly dependent, contradicting that V is in general position.

Combining (10.13) and (10.14), $f_j(\vec{a}_i) = \prod_{\vec{v} \in B_j} \vec{v} \cdot \vec{a}_i = 0$ if and only if there exists $\vec{v} \in B_j$ such that $\vec{v} \cdot \vec{a}_i = 0$ which is equivalent to say that there exists $\vec{v} \in B_j \cap A_i$, i.e., $A_i \cap B_j \neq \emptyset$. Thus we get the following

$$\begin{cases} f_j(\vec{a}_i) = 0, \text{ for any } i < j, \\ f_i(\vec{a}_i) \neq 0, \text{ for any } i. \end{cases}$$

By Lemma 10.19, we now see that $f_1, ..., f_m$ are linearly independent. ∎

10.6 Covering by Complete Bipartite Subgraphs

Problem. Determine the minimum $m = m(n)$ such that the edge set $E(K_n)$ of a clique K_n can be partitioned into a disjoint union of edge sets of m complete subgraphs of K_n.

Fact 10.38. $m(n) \leq n - 1$.

Proof. Because we can express $E(K_n)$ as a disjoint union of $n-1$ stars. ∎

We remark that there are more than one way to partition $E(K_n)$ into $n-1$ complete bipartite subgraphs.

Theorem 10.39 (Graham-Pollak)**.** $m(n) = n - 1$.

Proof. Suppose that $E(K_n) = E(B_1) \cup E(B_2) \cup \cdots \cup E(B_m)$, where $B_1, B_2, ..., B_m$ are complete bipartite subgraphs on $[n]$. We want to show that $m \geq n-1$. Let X_i and Y_i be the two parts of B_i. For B_k, we define an $n \times n$ matrix $A_k = (a_{ij}^{(k)})_{n \times n}$ by

$$a_{ij}^{(k)} = \begin{cases} 1, \text{ if } i \in X_k \text{ and } j \in Y_k, \\ 0, \text{ otherwise.} \end{cases}$$

It is clear to see that $rank(A_k) = 1$ for any k. Let $A = \sum_{k=1}^{m} A_k$, implying $rank(A) \leq \sum_{k=1}^{m} rank(A_k) = m$. Then $A + A^T = J_n - I_n$, where $J_n = (1)_{n \times n}$, because each $ij \in E(K_n)$ belongs to exactly one of the graphs B_k, where we have $a_{ij}^{(k)} = 0$ and $a_{ji}^{(k)} = 1$ or $a_{ij}^{(k)} = 1$ and $a_{ji}^{(k)} = 0$. It suffices to show that $rankA \geq n-1$.

Suppose for a contradiction that $rankA \leq n-2$. Let A' be the $(n+1) \times n$ matrix obtained from A by adding an extra row $(11 \cdots 1)$, so $rank(A') \leq n-1$. Then there exists a non-zero vector $\vec{x} \in \mathbb{R}^n$ such that $A'\vec{x} = \vec{0} \in \mathbb{R}^{n+1}$, which is equivalent to $A\vec{x} = \vec{0} \in \mathbb{R}^n$ and $\vec{1} \cdot \vec{x} = 0$, where $\vec{x} = (x_1, ..., x_n)$. Consider $\vec{x}^T(A + A^T)\vec{x} = \vec{x}^T(J_n - I_n)\vec{x}$ implying that $0 = \vec{x}^T J_n \vec{x} - \vec{x}^T \vec{x} = 0 - \sum_{i=1}^{n} x_i^2 < 0$, a contradiction. This proves that $n - 1 \leq rankA \leq m$. ∎

11 Finite Projective Plane (FPP)

Definition 11.1. *Let X be a finite set and $\mathcal{L} \subseteq 2^X$ be a family. The pair $(X, \mathcal{L})$ is called a finite projective plane (FPP for short) if it satisfies the following three properties.*

(P0) There exists a 4-set $F \subseteq X$ such that $|F \cap L| \leq 2$ for any $L \in \mathcal{L}$.

(P1) Any two $L_1, L_2 \in \mathcal{L}$ has $|L_1 \cap L_2| = 1$.

(P2) For any two $x_1, x_2 \in X$, there exists exactly one subset $L \in \mathcal{L}$ with $\{x_1, x_2\} \subseteq L$.

We call the elements of X as points, and the sets in $\mathcal{L}$ as lines. Let us explain the three properties:

- (P0) is used to exclude some non-interesting cases.
- (P1) says that any two lines intersect at exactly one point.
- (P2) says that any two points determine exactly one line.

Example 11.2 (The Fano plane (the smallest FPP))**.** *Where the set $X = [7]$ has 7 points and the set $\mathcal{L}$ has 7 lines with $\mathcal{L} = \{\{1,2,3\}, \{3,4,5\}, \{1,5,6\}, \{1,4,7\}, \{2,5,7\}, \{3,6,7\}, \{2,4,6\}\}$.*

Proposition 11.3. *Let $(X, \mathcal{L})$ be a FPP. Then any two lines $L, L' \in \mathcal{L}$ satisfy $|L| = |L'|$.*

Proof. We claim that there exists a point $x \in X$ with $x \notin L \cup L'$. To see this, let $F \subseteq X$ be from $(P0)$. Then $|F \cap L| \leq 2$, $|F \cap L'| \leq 2$. So we may assume that $F = \{a, b, c, d\}$ and $F \cap L = \{a, b\}$, $F \cap L' = \{c, d\}$. Let $\overline{ac}$ denote the line in $\mathcal{L}$ containing a and c; similarly, define $\overline{bd}$. Let $z \in \overline{ac} \cap \overline{bd}$ be the unique point. If $z \notin L \cup L'$, then we are done. So we may assume $z \in L$, i.e., $z \in L \cap \overline{ac}$. But $a \in L \cap \overline{ac}$, which implies that $z = a$. But again, we see $a, b \in L \cap \overline{bd}$, a contradiction.

For any point $\ell \in L$, the line $\overline{x\ell}$ intersects with L' at the unique point, say $\ell' \in L'$. We define a mapping $\phi : L \to L'$ by letting $\phi(\ell) = \ell'$ for any $\ell \in L$. Next we show that ϕ is a bijection between L and L'. (Exercise) ∎

Definition 11.4. *Let $(X, \mathcal{L})$ be a finite projective plane. The order of $(X, \mathcal{L})$ is the number $|L| - 1$, for each $L \in \mathcal{L}$.*

Proposition 11.5. *Let $(X, \mathcal{L})$ be a FPP of order n. Then*

(1) For each $x \in X$, there are exactly $n + 1$ lines passing through x.

(2) $|X| = n^2 + n + 1$.

(3) $|\mathcal{L}| = n^2 + n + 1$.

Proof. (1). Consider $x \in X$. Let F be the 4-set satisfying $(P0)$. Let $a, b, c \in F \backslash \{x\}$. Then, at least one of the lines $\overline{ab}, \overline{ac}$ which doesn't contain x (otherwise, a, b, c, x are in the same line). Let L be such a line with $x \notin L$. Let $L = \{x_0, x_1, ..., x_n\}$. Then $\overline{x_i x}$ define $n + 1$ lines. On the other hand, any line passing through x must intersect at some point say x_i. Thus, there are exactly $n + 1$ lines containing x.

(2). By (1), there are $n + 1$ lines $L_0, L_1, ..., L_n$ containing x. It is clear that $(L_i \backslash \{x\}) \cap (L_j \backslash \{x\}) = \emptyset$ for any $i \neq j$. Thus, $|L_0 \cup L_1 \cup \cdots \cup L_n| = n(n + 1) + 1 = n^2 + n + 1$. It is easy to see that $X = L_0 \cup L_1 \cup \cdots \cup L_n$.

(3). Let the incidence graph of a FPP $(X, \mathcal{L})$ be the bipartite graph with two parts X and L, where $x \in X$ is adjacent to $L \in \mathcal{L}$ if and only if $x \in L$. This defines an $(n + 1)$-regular bipartite graph. So $|\mathcal{L}| = |X| = n^2 + n + 1$. ∎

Definition 11.6. *The* incidence graph *of a FPP* $(X, \mathcal{L})$ *is a bipartite graph* G *with parts* X *and* $\mathcal{L}$*, where* $x \in X$ *and* $L \in \mathcal{L}$ *are adjacent in* G *if and only if* $x \in L$.

Definition 11.7. *The* dual $(\mathcal{L}, \wedge)$ *of a FFP* $(X, \mathcal{L})$ *is obtained by taking the incidence graph* G *of* $(X, \mathcal{L})$ *and interpreting the points in* $(X, \mathcal{L})$ *as the lines in the new FPP and the lines in* $(X, \mathcal{L})$ *as the points in the new FPP.*

Remark 11.8. *For any* $x \in X$*, let* $L_x = \{L \in \mathcal{L} : x \in L\}$ *be a new line in* $(\mathcal{L}, \wedge)$*. So* $\wedge = \{L_x : x \in X\}$.

Proposition 11.9. *The dual* $(\mathcal{L}, \wedge)$ *of any FPP* $(X, \mathcal{L})$ *of order* n *is also a FPP of order* n.

Proof. We point out that $(P1)$ for $(X, \mathcal{L})$ gives rise to $(P2)^*$ for $(\mathcal{L}, \wedge)$ and $(P2)$ for $(X, \mathcal{L})$ gives rise to $(P1)^*$ for $(\mathcal{L}, \wedge)$.

$(P1)$: For any $L_1, L_2 \in \mathcal{L}$ satisfying $L_1 \cap L_2 = \{x\}$ for some $x \in X$.

$(P2)$: For any two points $x_1, x_2 \in X$ there exists exactly one subset $L \in \mathcal{L}$ with $\{x_1, x_2\} \subseteq$ Ł.

$(P1)^*$: For any two points $x_1, x_2 \in X$ there exists exactly one subset $L \in \mathcal{L}$ with $\{x_1, x_2\} \subseteq$ Ł

$(P2)^*$: For any $L_1, L_2 \in \mathcal{L}$ satisfying $L_1 \cap L_2 = \{x\}$ for some $x \in X$.

We consider $(P0)^*$ for $(\mathcal{L}, \wedge)$.

$(P0)^*$: There exist four new points in $(\mathcal{L}, \wedge)$ such that any three of them cannot be contained in a new line of $(\mathcal{L}, \wedge)$, i.e., there exist $L_1, L_2, L_3, L_4 \in \mathcal{L}$ such that no L_x contains any three of them if and only if there exist $L_1, L_2, L_3, L_4 \in \mathcal{L}$ such that no three of them contain a point $x \in X$.

Consider the 4-set $F = \{a, b, c, d\} \in (X, \mathcal{L})$ satisfying $(P0)^*$. Note that $|F \cap \mathcal{L}| \leq 2$ for any $L \in \mathcal{L}$, So we have four distinct lines $L_1 = \overline{ab}, L_2 = \overline{cd}, L_3 = \overline{ac}, L_4 = \overline{bd}$.

It is easy to check that these four lines satisfy $(P0)^*$. ∎

Theorem 11.10. *A FPP of order* n *exists whenever a field with* n *elements exists.*

And we know that a field with n elements exists if and only if $n = p^k$ for a prime p.

Open Conjecture. A FPP of order n exists if and only if n is a power of a prime.

We know this holds for $n \leq 11$. In particular, FPP of $n = 10$ does not exist. It is open for $n = 12$.

Next we introduce an application of FPP in Turán numbers. Recall the following result.

Theorem 11.11. *Any* m*-vertex* C_4*-free graph* G *has* $e(G) \leq \frac{m}{4}(1 + \sqrt{4m - 3})$.

Theorem 11.12. *For infinitely many integers* m*, there exists a* C_4*-free graph on* m *vertices with at least* $0.35m^{3/2}$.

Proof. Take any FPP $(X, \mathcal{L})$ of order n, and consider its incidence graph G. Note that G has $m = 2(n^2 + n + 1)$ vertices and

$$e(G) = (n^2 + n + 1)(n + 1) \geq (n^2 + n + 1)^{\frac{3}{2}} = (\frac{m}{2})^{\frac{3}{2}} \geq 0.35m^{3/2}.$$

It is clear that G is C_4-free by the property of FPP. ∎